Chapter XII

Principles for Managing Information Security in the New Millennium

Gurpreet Dhillon
University of Nevada, Las Vegas

Previous chapters in this book have focused on identifying problems and challenges in managing information security in various contexts. The focus of this concluding chapter is to present a synthesized framework for managing information security in the electronic years. It is important to develop such a conceptual understanding since the challenges of managing information security permeate various aspects of our personal and business life. Whether it may be booking flights over the Internet, buying a book or simply browsing to gather information, challenges to protect personal information exist and there are simply no straightforward answers. Similarly for businesses, protection of information is absolutely critical. Obviously no company would like, for example, its competitors to have access to their sales data. Or for that matter, companies would neither appreciate unauthorized use of computers by their employees nor would a violation of safeguards by trusted personnel go down very well. For these reasons it is important that companies consider certain fundamental principles that could be used as pointers for not only establishing an information security vision and strategy, but would also facilitate in mapping out a detailed security policy.

This chapter sketches out three classes of principles. Following a brief description of the class, each principle is elaborated and suggestions made thereof as to its applicability. The three classes of principles are:

- Principles for managing the pragmatic aspects of an organization.
- Principles for managing the formal rule-based aspects of an organization
- Principles for managing the technical systems


PRINCIPLES FOR MANAGING THE PRAGMATIC ASPECTS

The various chapters and studies presented in this book, particularly the analysis of prescription fraud in the British National Health Services Pouloudi (2001), suggests the importance of broader social and organizational issues in managing information security concerns. Pouloudi (2001) argues that a particular context may make fraud a legitimate activity. Therefore it is important to understand the context in which an information technology is being implemented. She further suggests that by carefully interpreting issues and concerns of various stakeholders, it is possible to understand the interaction between technical and social aspects of an information technology implementation, thus facilitating fraud prevention. Research done by Dhillon and Backhouse (1996) is also in a similar vein. By evaluating the unethical computer use practices of Jett at Kidder Peabody, it is suggested that it is important to inculcate a culture of trust and responsibility. It becomes apparent therefore that organizations need to develop a focus on the pragmatic aspects in managing information system security. The various principles that need to be adopted are as follows.

Principle 1: Education, training and awareness, although important, are not sufficient conditions for managing information security. A focus on developing a security culture goes a long way in developing and sustaining a secure environment. Research has shown that although education, training and awareness are important in managing the security of enterprises, unless or until an effort to inculcate a security culture exists, complete organizational integrity will be a farfetched idea. Dhillon (1997) has suggested that “a mismatch between the needs and goals of the organization could potentially be detrimental to the health of an organization and to the information systems in place…. organizational processes such as communications, decision making, change and power are culturally ingrained and failure to comprehend these could lead to problems in the security of information systems” (p. 111). While discussing issues in disaster recovery planning, Adam and Haslam (2001) note in an earlier chapter that although managers are aware of the potential problems related with a disaster, they tend to be rather complacent in taking any proactive steps. Such an attitude could be a consequence of the relative degree of importance placed on revenue generation. As a consequence, while automating business processes and in a quest for optimal solutions, backup and recovery issues are often overlooked.

Principle 2: Responsibility, integrity, trust and ethicality are the cornerstones for maintaining a secure environment. In Chapter 1 we noted that given that the nature of organizations has evolved from a predominantly hierarchical organization to a more networked form, traditional security models and approaches fall short of developing secure environments. Dhillon and Backhouse (2000) have argued that traditional “information security principles of confidentiality, integrity and availability are fine as far as they go, but they are very restricted”. In response to the changing organizational contexts they suggest the RITE (responsibility, integrity, trust and ethicality) principles. The RITE principles hark back to an earlier time period when extensive reliance on technology for close supervision and control of dispersed activities was virtually non-existent. Beniger (1986) terms this as the ‘factorage system of distributed control’ where the trade between cotton producers in America and British merchants was to a large extent based on trust (pp. 132-133). The extensive reliance on information technologies today questions the nature and scope of individual responsibilities and many times challenges the integrity of individuals. Trust is