Chapter XVII
Theories Used in Information Security Research: Survey and Agenda

Serkan Ada
State University of New York, USA

Raj Sharman
State University of New York, USA

Manish Gupta
State University of New York, USA

ABSTRACT

This chapter discusses the recent theories used in information security research studies. The chapter initially introduces the importance of the information security research and why it became so important recently. Following this introduction, “theory” is defined and the importance of the theories in information security research is mentioned. After this discussion, recently used theories (socio-technical systems theory, activity theory, distributed cognition theory, general deterrence theory, grounded theory, social cognitive theory) are listed and basic information about these theories as well as applications from the literature are given. Other recently used theories are also summarized in a table in the next section. The chapter finally ends with concluding remarks on the theories and recommendations to the researchers in the information security area.

INTRODUCTION

In today’s global and competitive business environment, organizations are becoming increasingly dependent on information and dissemination of the information. Such being the case, the use of computer-based information systems as well as globally scattered computer networks is of great importance in order to meet these requirements. On the other hand, this dependency makes or-
organizations’ information systems progressively more vulnerable to outside attacks and/or internal security breaches which may cause financial losses and disruption of the business activities (Siponen, 2005) (Choobineh et al., 2007).

In order to better comprehend the significance of the problems mentioned above, it is beneficial to take a look at the findings of the recent study conducted by Computer Security Institute. According to this study (CSI Survey, 2007), 46% of the 487 survey respondents reported that their organization was exposed to at least one security incident in the past 12 months. Another very significant statistic shows that organizations’ total financial losses due to computer security incidents are approximately $66,930,950 in 2007 (based on the responses from managers of 194 companies). More interestingly, 27% of the respondents also reported that up to 20% of the cyber losses is caused by the people inside the organization, while this proportion is 37% for the cyber losses greater than 20% (Richardson, 2007). In light of the findings, as mentioned above, it is obvious to conclude that proper management of information systems security is vital and inevitable. In addition to this very fact, it is also of great importance for academic environments to attach more importance to the information security related issues in organizations.

How academic environments approached these issues are summarized in a review paper on Information Security Research (Willison & Siponen, 2007). This study reports that there are 1280 security related papers published in 3 IS Security journals and 20 IS journals between 1990-2004. Out of these papers, only 18.51% include a theory as a framework the study. Based on the fact that the application of the theories and appropriate research methods are essential for any research study, it is our belief that academic researchers should attach more importance on the creation, adoption, and/or application of the theories from the literature (Willison & Siponen, 2007). Drake and Clarke (2008) also offer a model to suggest solutions and guidelines to fill the information security research gaps by using social theories, various aspects of which deal with both human and technical issues from the perspective of those involved in the system of concern.

In this chapter, it is our objective to present some of the related theories used in the context of Information Security in order to bring this issue to the academic researchers’ notice. As also mentioned by Choobineh et al. (2007), theoretical conceptualizations are necessitated in order to create more effective principles and guidelines for “best practices” in information security management and to develop solutions for the related problems (Choobineh et al., 2007). Because of this, we would like to encourage researchers to utilize these theories or adopt other related theories from the literature for their research studies.

The remaining of this chapter is organized as follows. The next section discusses what the theory is and why the theories are used in research studies. Following this section, we will discuss the related theories used in Information Security Research (Socio-technical Systems Theory, Activity Theory, Distributed Cognition Theory, General Deterrence Theory, Grounded Theory, and Social Cognitive Theory). After discussion of these theories, other recent theories used in the literature will be briefly mentioned. Finally, the chapter will conclude with the conclusion and discussion section.

**THEORY AND ITS APPLICATION IN INFORMATION SECURITY**

Theory is defined by Kerlinger (1979) as “a set of interrelated variables, definitions, and propositions that presents a systematic view of phenomena by specifying relations among variables, with the purpose of explaining natural phenomena.” (Creswell, 2003). Another definition of the theory is done by Babbie (2004) as “a systematic explanation for the observations that relate to a particular