Chapter XVIII
Security Requirements Elicitation: An Agenda for Acquisition of Human Factors

Manish Gupta
State University of New York, Buffalo, USA

Raj Sharman
State University of New York, Buffalo, USA

Lawrence Sanders
State University of New York, Buffalo, USA

ABSTRACT

Information security is becoming increasingly important and more complex as organizations are increasingly adopting electronic channels for managing and conducting business. However, state-of-the-art systems design methods have ignored several aspects of security that arise from human involvement or due to human factors. The chapter aims to highlight issues arising from coalescence of fields of systems requirements elicitation, information security, and human factors. The objective of the chapter is to investigate and suggest an agenda for state of human factors in information assurance requirements elicitation from perspectives of both organizations and researchers. Much research has been done in the area of requirements elicitation, both systems and security, but, invariably, human factors are not been taken into account during information assurance requirements elicitation. The chapter aims to find clues and insights into acquisition behavior of human factors in information assurance requirements elicitation and to illustrate current state of affairs in information assurance and requirements elicitation and why inclusion of human factors is required.

INTRODUCTION

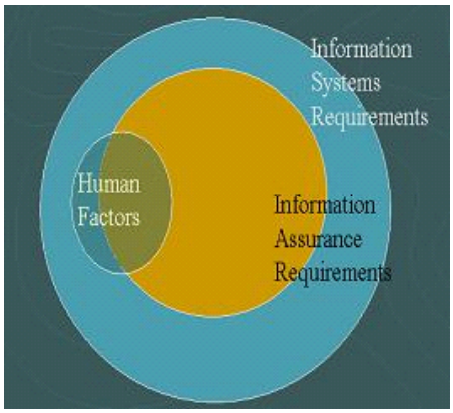
In last few years, information security has attained a very important position in organizations and personal lives. A decade ago, it was very uncommon for colleges to offer any course in information security, privacy, or information assurance. In 2005, the U.S. National Security Agency certified 67 academic institutions as Centers of Academic Excellence in Information Assurance Education, which evidently underscores the importance of security of information in everyone's lives as corporate citizens and as individuals. However this has arisen to another interesting assumption that computer security is primarily a technical subject. This ignores the fact that computer security's technical aspects are only as effective as people designing, using, attacking, and protecting information systems. People are the cornerstone of information security and privacy. Security solutions that fail to take human factors into account are not going to be effective in protecting information systems or providing any assurance thereof. Schwartz (2005) quoted a survey finding that "89% of respondents believe major security breaches have been reduced as a result of IT security training and certification." According to the survey, the perceived benefits of training include "improved potential risk identification, increased awareness, improved security measures, and an ability to respond more rapidly to problems."

The chapter aims to investigate and suggest an agenda for state of human factors in information assurance requirements elicitation from perspectives of both organizations and researchers. For any project or information system implementation, requirements elicitation is one of the most important steps. Information security requirements have been long introduced as a vital component of overall requirements elicitation. Much research has been done in that area, as is also discussed in a following section. But, invariably, human factors are not been taken into account during information assurance requirements elicitation. The chapter aims to find clues and insights into *acquisition behavior of human factors in information assurance requirements elicitation and to illustrate current state of affairs and importance of human factors of information assurance and requirements elicitation.* This chapter, based on survey and synthesis of existing literature, aims to bring out the current state of affairs in that area and also suggests why this is vitally critical for success of the information systems usage, more so, in light of growth of exploitation of human factors to manipulate and invalidate information systems.

SYSTEMS AND SECURITY REQUIREMENTS ELICITATION: HUMAN FACTORS

More often than not, it is becoming increasingly evident that the weakest links in an information-security chain are the people, because human nature and social interactions are much easier to manipulate than targeting the complex technological protections of information systems. Concerns and threats regarding human and social factors in organizational security are increasing at an exponential rate and shifting the informa-

Figure 1. Research coverage and areas



Related Content