Chapter X

Information Security Risk Analysis: A Pedagogic Model Based on a Teaching Hospital

Sanjay Goel, University at Albany, SUNY, and NYS Center for Information Forensics and Assurance, USA

Damira Pon, University at Albany, SUNY, and NYS Center for Information Forensics and Assurance, USA

Abstract

There is a strong need for information security education, which stems from the pervasiveness of information technology in business and society. Both government departments and private industries depend on information systems, as information systems are widespread across all business functions. Disruption of critical operational information systems can have serious financial impacts. According to a CSI/FBI report (2004), losses from security breaches have risen rapidly in recent years and exceeded $200 million in 2003. The information security field is very diverse and combines disciplines such as computer science, business, information science, engineering, education, psychology, criminal justice, public administration, law, and accounting. The broad interdisciplinary nature of information security requires several specialists to collaboratively teach the curriculum and integrate different perspectives and teaching styles into a cohesive
delivery. This chapter presents a pedagogical model based on a “teaching hospital” concept that addresses the issues introduced above. By using a specific information-risk-analysis case, the chapter highlights the basic concept of the teaching hospital and its application in teaching and learning contexts.

Learning Objectives

After completing this chapter, you will be able to:

- Discuss the issues associated with information assurance education.
- Describe the basic concept of teaching hospital approach in information security risk analysis.
- Understand the case development methodology used to support the teaching hospital.
- Suggest possible improvements to the cases described in the chapter.

Introduction

Information assurance (IA) is a complex field, especially due to the dynamically changing security environment and constant evolution of practices and procedures. It is difficult to provide training in such an area since material developed becomes obsolete very quickly. To develop a better understanding of IA, concepts should be assimilated from several disciplines (i.e., computer and information science, law, business, etc.) and blended into the context of real problems. In this chapter, a teaching hospital model that has been developed for IA training in the context of information security risk analysis is described. The teaching hospital approach involves incorporating real cases to supplement existing curriculum, which keeps teaching material relevant over time through infusion of current research problems in the curriculum and creates a rich learning environment that is both stimulating and dynamic. The New York State Center for Information Forensics and Assurance (CIFA) at the University at Albany has developed a teaching hospital for IA education (Goel & Pon, 2005). Within this teaching hospital, a research program that solves current industry problems is combined with a teaching program responsible for dissemination of curriculum. Problems from public and private sector organizations are intro-