IDEA GROUP PUBLISHING **ITB11404**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the book, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* by Lech J. Janczewski and Andrew Colarik © 2005, Idea Group Inc.

Chapter 1

Information and Computer Security

The current state of the information security domain in the United States and much of the rest of the industrialized world can best be characterized as overly optimistic. The protection of computing systems and telecommunication infrastructures from unauthorized usage, manipulation, and sabotage faces serious challenges to ensure ongoing serviceability. This is especially true when we consider our growing dependence on these infrastructures. The state of affairs regarding the security aspects of these systems is even worse. Peter G. Neumann of the Computer Science Laboratory at SRI International in Menlo Park, California states:

> *There is a seemingly never-ending stream of old and new security flaws, as well as markedly increased security threats and risks, such as viruses, Trojan horses, penetrations, insider misuse, identity theft, and fraud. Today's systems, applications, and networking tend to largely ignore security concerns—including such issues as integrity, confidentiality, availability, authentication, authorization, accountability, and the spread of malicious code and e-mail spam—and would-be attackers and misusers have significantly wider knowledge and experience. Moreover, there is a general naiveté whereby many people seem to believe that*

> *technology is the answer to all security questions, irrespective of what the questions are.*
>
> *In addition to security concerns, there are serious problems relating to system dependability in the face of a wide range of adversities. Such adversities include not only misuse but also hardware malfunctions, software flaws, power disruptions, environmental hazards, so-called "acts of God," and human errors. The nation seems to have evolved into having a rather blind faith in technologies that often are misunderstood or misapplied, and into placing trust in systems and the people involved with them, even though they have not proven entirely trust "worthy".* (http://www.nap.edu/issues/19.4/neumann.html)

This perspective regarding the state of security seems quite negative on the surface but serves as a point of reference for focusing efforts on resolving some of the more predominant security issues that face us today. Before proceeding further on the discussion of security, we need to have a shared understanding of the core fundamentals, distinctions, and definitions that comprise information security. Therefore, we start this chapter with the essential security definitions followed by an historical brief in order to begin further discussions from the same reference points. An outline of implementing information security principles in an efficient manner is also presented, and we conclude this chapter with our assessment of the current state of affairs in the field of information security.

Definitions

For the purpose of defining the core information security concepts, we shall draw on those suggested by D. Gollmann and based on the ITSEC Evaluation Criteria. Gollmann states that information security covers the following:

- Confidentiality. The prevention of unauthorized disclosure of information. Traditionally, confidentiality meant *controlled access to information*. This term means that the access to data is a function of the person seeking access and the type of access. For one person, access could be *read only*, and for others it could be *read and write*. Other access rights can be formulated as well.