IDEA GROUP PUBLISHING
ITB11416
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 13

Information Security Policy

In Chapter 12, we discussed most of the information security issues that are important to IT managers, especially in the current situation of increased attacks. Perhaps the most visible and important document that relates to the attitude of management towards security issues is the Information Security Policy (ISP). (Please note that the most common understanding of the abbreviation *ISP* is Internet Services Provider. For clarity within *this* chapter *only*, ISP means Information Security Policy.) This document reflects all the decisions and activities required to set up a clear set of rules and procedures for company employees in terms of protecting information assets. The ISP is also used to:

- Place security on an equal footing with all of the other company's business issues.
- Demonstrate top management support for the protection of company information.
- Create a security-conscious atmosphere within the company.
- Provide proactive preparation against possible lawsuits based on breaches of laws, such as privacy acts or contractual obligations like confidentiality agreements.

To function properly, the ISP document must be based on the company's general business policy. The ISP document should exist in three different formats.

- General ISP Policy. A general ISP policy may be a very short document (i.e., less than one page) stating that the security of information is important to the company, and that all staff members are responsible for assuring that data will be accessible only to those authorized, and not changed without authorization. More or less, it is an ISP mission statement.
- Practical ISP Rules. Practical ISP rules is a collection of basic rules on how to handle company documents and resources in order to maintain a high level of security. These rules are top-level concepts of security dos and don'ts. For instance, it could contain a statement that all company files need to have backups performed at the end of each working day, or that no staff member is allowed to disclose his or her password to anyone, and so forth. Practical ISP rules usually are a few pages in length. It is a good custom to present this document to all employees and to ask them to sign an acknowledgment.
- Detailed ISP Procedures. A detailed ISP procedures document is an extension of the practical rules and contains details of all the procedures mentioned in the practical ISP rules document. It is also a detailed instructional breakdown of those rules (i.e., how to do a proper backup). Obviously, the development of such a document can have an initial cost, but once created, it can provide a basis for employee training and consistency.

The practical ISP rules are perhaps the most important part of the ISP, and the rest of the chapter will concentrate on this. Because of the variations in hardware, software, and network infrastructures, we must defer the detailed procedures for internal development on a company-by-company basis. Just keep in mind that such procedures will come from a thorough rules document.

An ISP should address a number of issues, and the following seem to be the most important (not necessarily in any order of importance).

- Secure communications. Any issues related to the importing and/or exporting of data from the company is a process to which access should be given only to authorized persons and systems.