IDEA GROUP PUBLISHING ITB11415

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 12

Operations Management

A major focus of this book is guiding IT managers on how to secure the operations of their facilities due to increased threats from terrorist oriented attacks. As it was presented in the earlier part of the text, there are many procedures that would decrease such threats. However, the best protection is just to run the facilities, keeping in mind the systems approach to information security. In this way, we are able to optimize the protection of the workplace from any form of attack, including those from cyber-warriors and cyber-terrorists. In this chapter, we will present the essence of managing IT facilities from the security point of view.

Operational Procedures and Responsibilities

The rational management of IT facilities is based on carefully prepared and implemented documentation of all operating procedures. Among those tasks are instructions about information processing, as well as the scheduling of jobs, advice on how to handle emergencies, location of help desks in case of errors, handling results, and so forth. It is important that these instructions be kept current and regularly updated. Especially important are the solution sets for handling emergencies.

In setting up the operational procedures, it is very important to arrange the segregation of duties. The essence of this is that the operator should not be the one benefiting from the operation. An example of this is that the designer of a payroll system should not be on an access list that distributes checks to employees. This is well illustrated by a case that happened many years ago at a university in the United Kingdom (Case 12.1).

While this example is not earth threatening, it illustrates what may become a tremendous issue when an individual seeks to be harmful. Subversive coding can sometimes be extremely difficult to discover. One such example of this approach to system disruption is called a *salami attack*. The programmer introduces into the system design a counter or collector of changes. If these changes reach a setup limit, this routine launches a series of unauthorized activities. The trick to these types of attacks is that a series of events must occur over time before anything happens.

The classic example of a salami attack is preserving the remainder of financial transactions such as pay calculations. These remainders are accumulated and forwarded to an account for later disbursement. While the amounts appear to be fractions of a cent, their accumulation can become sizeable over time. The only way to discover such an attack is to monitor deposit transactions. It is precisely why segregation of duties is critical to auditing actions and transactions that such attacks can be prevented.

Case 12.1: Disgruntled programmer

A British University had a computer that was used for administration purposes. With more and more advanced equipment available, fewer jobs were being processed on this machine. Finally, only one faithful man remained to run the machine. The computer was processing only a small part of the financial transactions of the University. But as time passed, the man was eventually discharged. Obviously, he was not very happy about it and promised revenge. During the next run after his departure, the machine stopped and displayed a message to the surprised operator: "The Phantom Strikes Again." Upon restarting the process, the program ran without a problem. This harmless bug reoccurred at random until the machine was finally retired. It just was not economically feasible to hunt for the coding of the bug.