IDEA GROUP PUBLISHING ITB11417

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 14

Business Continuity Management

Business continuity management is a process aimed at reducing disruptions caused by disasters and security failures that could be the results of natural phenomena, accidents, failure of equipment, or deliberate human acts. Among the last of the results are cyber-terrorist attacks or acts of information warfare.

A long time ago, it was proven that the present level of technology allows for the elimination of pilots from the cockpits of large commercial jets. A huge jumbo jet is able to take off, fly to the opposite side of the globe, and land safely without human intervention. With this knowledge, we must wonder why airline pilots spend so much time on flight simulators, and why pilots are still needed in the front of the plane. The answer is really quite simple: they are rigorously trained to handle emergency situations.

The same approach to emergency preparation applies to IT. In these times of terrorism, we need to design and implement plans on how to react in such crises, and what to do to minimize the possible results of attacks against the information resources of an organization.

In Chapter 3, we discussed the possibilities of being hit by a terrorist or cyber-terrorist attack. Let us summarize here again the main points of this discussion.

- The most probable form of any attack is being infected by a computer virus. According to every available survey, only a small number of systems have never faced such a threat.

- The next most popular threat is the theft of laptops, which may result in providing an access point into a company, furnishing critical security data, or losing confidential information.
- The probability of disasters like floods and fire is next on the list of possible threats. Depending on the location of your organization, other natural disasters must be considered (i.e., earthquakes or tsunamis).
- The probability of a cyber-terrorist attack depends largely on the public profile that your organization maintains. It is obvious, as it was mentioned before, that government or military agencies are primary targets, but any well known organization could be such a target (well known international corporations, in particular).
- If your IT facilities are servicing or located near a government, military, or other highly sensitive operation, then there is a high chance of collateral damage resulting from conventional terrorist attacks against the organization. This also depends on where the operation is located. Currently, the Middle East is perhaps the most dangerous zone.

A decade ago, a large earthquake shook Kyoto, Japan. Significant parts of the downtown were totally destroyed. It is estimated at that time that about 20% of businesses did not survive the quake due to the destruction of their computer-located records. On the other hand, we read a report on actions taken by management of a major U.S. West Coast bank whose headquarters were destroyed in a fire. Within a day they were able to resume basic operations, and within a week resume all regular activities. This was made possible because management had prepared a solid business continuity management program.

Business Continuity Management Process

Preparation of a quality business continuity plan requires a systems approach consisting of three phases: