IDEA GROUP PUBLISHING ITB11406

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 3

Cyber-Terrorism

In this time of increased threats of terrorist attacks, are IT professionals really facing a new type of danger resulting from these activities? In our opinion, the answer is both *yes* and *no*. Let us explain.

Major information system users, such as government agencies, military installations, major banks, and so forth, were and are prepared for handling such attacks. The destruction of part of the Pentagon in Washington, D.C. did not stop the U.S. Department of Defense from functioning, nor did the collapse of the Twin Towers create a permanent crisis on Wall Street. The fact is, however, that trading on the New York Stock Exchange was suspended for some time, and many small companies with offices in the Twin Towers did not survive the disaster. But no long-term nationwide disruption was triggered, in an economical sense. Similar attacks have happened to other large corporations, and their consequences have been minimized through redundancy implementations and considerable resources. On the other hand, most businesses are small to medium sized and, as such, may not be prepared to handle terrorist threats due to the lack of resources (i.e., specialized skill sets, facilities, etc.).

The word *terrorism* brings to mind a picture of bearded men throwing a pouch filled with explosives. But in the context of IT security, terrorists can come in many forms, such as politically motivated anti-government, anti-world trade, and pro-environmental extremists. If given the opportunity, such activists would gladly disrupt trade and legislative meetings by attacking a facility's communications server, especially if the media were standing by to report what happened.

In previous chapters, we outlined the domains of information security and terrorism, and also demonstrated why they are important for IT managers. In this chapter, we will discuss how terrorism may influence the functioning of IT in a typical business organization. We also will present the most important activities that need to be undertaken by an IT manager to handle this new type of threat.

Possible Terrorist Activities Against IT

Terrorist activities can have an impact on IT in three primary ways.

1. Direct attack on IT facilities. The probability of launching a direct attack on IT facilities depends on the nature of those facilities; that is, the more important they are, the higher the chance that they could be targeted. The most probable result of a terrorist attack on IT facilities would be at least a temporary suspension of the regular workload of those facilities. Depending on the direct goal of the attackers, the consequences could range from amusing to deadly. The amusing sort (i.e., annoyance) consists of changes to Web pages, such as changing a corporate motto from "The Most Experienced Company" to "The Most Unexperienced Company." While this attack creates some image difficulties, it is relatively non-life threatening. On the other end of the scale, changes to information systems that control human lives could be dire. Discussions about cyberattacks on critical infrastructures such as air traffic control systems and the electrical power grids throughout the world (e.g., the SCADA systems) are important. But there is also a host of smaller attacks that have focused consequences. Imagine the situation where an important or wealthy person is undergoing open-heart surgery at a hospital or specialized clinic, and a terrorist manages to crash the computerized equipment being used or supporting the operating theatre. Therefore, installation and operations secrecy becomes an important defence against such attacks.
2. Collateral IT damages resulting from terrorist attacks against other targets. Terrorist attacks may take a physical form in the use of explosives to blow up a structure (i.e., a building, a motor vehicle, etc.). Such an attack creates collateral damage to the IT infrastructure and installations. In the aftermath of the destruction of the Twin Towers in New York, many