IDEA GROUP PUBLISHING **ITB11407**

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 4

Physical Security

The final stage in the execution of the majority of the current waves of terrorist attacks is in the form of an intruder positioning a bomb in the proximity of the target. While terrorists may not directly target IT systems, attacks against computer facilities do happen. These attacks are in addition to telecommunication-based attacks and fall into the realm of physical security.

Case 4.1: Wanganui Computer Centre

In 1976, the Parliament of New Zealand passed a law entitled the Wanganui Computer Centre Act. The Act laid the foundation to build a powerful computing facility in the city of Wanganui (hence the name of the Act) for supporting the activities of the New Zealand Police. The main idea behind the project was to create a databank on criminals and their particular offenses in order to help the police with enforcement and prevention activities.

The designers of the facility understood the importance of the data that would be stored and processed at the facility and, as such, made provisions for physical security measures. In 1982, Neil Roberts, a 22 year old anarchist punk rocker, detonated a bomb he was carrying at the doors of the facilities. The damages were restricted to the reception area. The operation centre was undamaged and uninterrupted as a direct result of the designers' security measures.

Before we can establish physical security measures, let us first understand the areas of concern and identify what we consider to be the most important aspects of the physical security domain. Our explanation of physical security, as it applies to information security, considers the activities undertaken and the equipment installed to accomplish the following objectives:

1. Protection against unauthorized persons to penetrate the designated off-limit areas of the company premises. This definition implies that there may be several classes of unauthorized persons, and the company premises may have security zones with different access rights. Some areas, such as the reception area, could be open to virtually anyone, while other areas might be accessible only to a limited number of company employees.
2. Protection against the theft of company IT equipment, especially that containing sensitive information. This protection extends to company equipment that may be physically outside of the company's premises.
3. Protection against the physical destruction of company IT equipment. This can include the protection against such acts as the planting of explosives within the company premises. This also covers the protection measures against such events as fire, floods, and earthquakes.
4. Protection against the unauthorized reading of information, regardless of its form (i.e., visual, acoustic, or analogue signals). Security measures must prevent unauthorized persons from reading sensitive data from a computer screen from intercepting spoken messages, from tapping telephone lines, or similar acts.

The security measures discussed here do not include security breaches such as the unauthorized system access to data through a broken password subsystem or the breaking of a cryptographic message. It also does not cover breaches resulting from wrongly deployed mobile telecommunications systems, such as a mobile Local Area Network. We will discuss this area in further detail later in the book.

In our presentation of physical security, we shall follow the OECD recommendations that relate to Proportional Control measure. The OECD measures are based on common sense and human psychology. This particular principle means that our defenses should be appropriate to resources that they are