IDEA GROUP PUBLISHING
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
ITJ2705

Information Technology as a Target and Shield in the Post 9/11 Environment

Laura Lally, Hofstra University, USA

ABSTRACT

This paper draws upon Normal Accident Theory and the Theory of High Reliability Organizations to examine the potential impacts of Information Technology being used as a target in terrorist and other malicious attacks. The paper also argues that Information Technology can also be used as a shield to prevent further attacks and mitigate their impact if they should occur. A Target and Shield model is developed, which extends Normal Accident Theory to encompass secondary effects, change and feedback loops to prevent future accidents. The Target and Shield model is applied to the Y2K problem and the emerging threats and initiatives in the Post 9/11 environment.

Keywords: computer privacy; computer security; normal accident theory; post 9/11; target and shield model; terrorism; theory of high reliability organizations; Y2K

INTRODUCTION

In the Post 9/11 environment, Information Technology (IT) Security has become a growing issue. Throughout the 1990s, the field of IT security faced a wide range of new challenges. Yourdon (2002) places these challenges in three categories:

1. More organizations are dependent on the Internet for day-to-day operations.
2. An increasing number of computer systems, networks and databases make up a global IT infrastructure. Individuals, organizations and nations are "increasingly 'wired,' increasingly automated and increasingly dependent on highly reliable computer systems." (p. 96)
3. IT managers face more sophisticated and malevolent forms of attacks on these systems. Unlike the Y2K problem, which was the result of an innocent bad judgment, "the disruptive shocks to our organizations are no longer accidental, benign or acts of nature; now they are deliberate and malevolent." (p. 205)

Furthermore, IT-based systems may not only be the targets themselves, they may be used as a weapon in attacks against other key infrastructure systems (National Research Council, 2002). Designing secure, resilient systems in the face of these new threats will be a major challenge for IT managers in the next decade. Robust methodologies will be needed to identify the sources of these threats, eliminate them if possible, contain their impact if they do materialize and prevent damage they cause from propagating further.

As the events of 9/11 illustrated, IT-based threats are not the only source of disasters, and IT-based systems not the only target of malevolent individuals. However, on 9/11, IT-based systems were used to mitigate the impacts of the damage and, as this analysis will indicate, could have done so to an even greater extent with proper design, implementation and training. This analysis will argue, therefore, that IT-based systems are not only a **target**, a source of vulnerability, but that they also can be a **shield**, a means of combating the threats and mitigating the damage malicious individuals are able to accomplish.

IT managers and educators, therefore, must face two new challenges:

1. How to design more secure, resilient IT-based systems in the future
2. How to use IT to combat threats to IT-based systems, as well as physical threats

To address these two issues, this research will develop a **"Target and Shield"** conceptual model of the sources; propagation and potential impacts of IT-related threats; and the means by which IT can be used to identify, eliminate and mitigate the damages caused by other sources of threats. The model will focus on:

1. how the current IT infrastructure allows for the propagation of IT-based threats;
2. means by which available IT tools can help identify potential IT-based threats and mitigate their impacts; and
3. means by which IT can be used to counter physical attacks.

The Y2K problem and the information technology implications of 9/11 will be used to illustrate the analysis. Implications for managers planning future IT-based systems, as well as for educators, will emerge from the analysis.

The conceptual model will draw on two theoretical perspectives, an extended version of Perrow's Normal Accident Theory and the Theory of High Reliability Organizations.

NORMAL ACCIDENT THEORY AND THE THEORY OF HIGH RELIABILITY ORGANIZATIONS

Normal Accident Theory argues that characteristics of a system's design make it more or less prone to accidents. Accidents are defined as "a failure in a subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system." (Perrow, 1984, p. 66) Perrow distinguishes between disastrous "accidents," which are system-wide and seriously impact the system's overall functioning, and "incidents," which involve single failures that can be contained within a limited area and do not compromise the system's overall functioning. Perrow argues that no system can be designed to completely avoid incidents, but that inherent qualities of the system determine how far and how fast the damage will spread. Systems that are not designed to contain the negative impact of incidents will, therefore, *be subject to accidents in the course of their normal functioning.*

The first key characteristic of accident-prone systems is their complexity. Normal Accident Theory argues that as systems become more complex, they become more accident prone. Normal Acci-