IGI PUBLISHING

ITB14765

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Emerging Information Resources Management and Technologies**
edited by **Mehdi Khosrow-Pour, DBA © 2007, IGI Global**

Chapter VII

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

Laura Lally, Hofstra University, USA

Abstract

This chapter 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 chapter also argues that information technology can 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. The model is then extended to encompass the use of IT as a weapon against terrorism.

Introduction: IT Initiatives in the Post-9/11 Environment

In the post-9/11 environment, information technology (IT) security has become a growing issue. Even though computer budgets are being cut, spending on security has increased. Funding for IT based initiatives has increased dramatically since 9/11. New government regulations require that organizations keep their systems more secure and keep better track of their documents. As a result, an increasing number of IT based initiatives have been developed to solve these problems.

MIT's Magazine of Innovation: Technology Review reports that the budget for the 2005 Department of Homeland Security was $30 billion dollars (MIT Editors, 2005). For Customs, Immigration, and Border Protection, it included $2.9 billion for container security and $340 million for U.S.-VISIT, an automated entry and exit system for frequent international travelers. For the Coast Guard, it included $724 million to upgrade the technology and communications division. For the Transportation Security Administration, it included $475 million for explosives detection systems, baggage screening equipment, and their installation. For state and local assistance programs, it included $150 million in port security grants, $150 million in rail/transit security grants, and $715 million in grants to fire departments. For the Emergency Preparedness and Response Directorate, it included $2 billion for an emergency relief fund. For the Science and Technology Directorate, it included $593 million to develop technologies that counter threats from chemical, biological, nuclear and radiological weapons, and high explosives, and $61 million to continue the development of innovative countermeasures to protect commercial aircraft against possible missile systems. For Information Analysis and Infrastucture Protection Directorate, it included $2 billion to assess and protect critical infrastructures including cyberspace.

This chapter proposes a theory based model for creating a taxonomy of these initiatives. The goals of the taxonomy will be (1) to increase interoperability among the initiatives, (2) to identify areas of basic IT research which support these new applications, and which may need to be developed further for the applications to be successful, (3) to identify additional applications of these initiatives, and (4) to identify potential privacy and civil rights violations that could result from the inappropriate use of these initiatives.