Chapter IX

Insights from Y2K and 9/11 for Enhancing IT Security¹

Laura Lally
Hofstra University, USA

Abstract

In the post-9/11 environment, there has been an increasing awareness of the need for information security. This chapter presents an analysis of the Y2K problem and 9/11 disaster from the perspective of Lally’s extension of Perrow’s Normal Accident Theory and the Theory of High Reliability Organizations. Insights into: 1) how characteristics of current IT infrastructures and organizational cultures make disasters more likely, 2) how organizations can respond to potential threats and mitigate the damage of those that do materialize, and 3) how IT can be used to identify future threats and mitigate their impact in the future, emerge from the analysis.
Introduction

In the post-9/11 environment, information technology managers have become more aware of the importance of security. Throughout the 1990s, 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” (Yourdon, 2002, p. 96).
3. IT managers faced more sophisticated and malevolent forms of attacks on these systems. Unlike the Y2K problem, which was the result of an innocent bad judgement, “the disruptive shocks to our organizations are no longer accidental, benign, or acts of nature; now they are deliberate and malevolent” (Yourdon, 2002, p. 205).

This chapter will present an analysis of the sources, propagation and potential impacts of IT related threats. The Y2K problem and the information technology implications of 9/11 will be used to illustrate the analysis. The analysis will focus on both: 1) how the current IT infrastructure allows for the propagation of IT based threats, and 2) ways in which available IT tools can help identify potential threats and mitigate their impact.

Extending Perrow’s Normal Accident Theory and the Theory of High Reliability Organizations

This analysis will draw on Lally’s (2002) extension of Perrow’s Normal Accident Theory (1984, 1999), as well as the Theory of High Reliability Organizations. Perrow developed his theory studying complex systems such as
Ensuring Privacy and Confidentiality in Digital Video Surveillance Systems
www.igi-global.com/chapter/ensuring-privacy-confidentiality-digital-video/61503?camid=4v1a

A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security
www.igi-global.com/article/a-hybrid-concept-of-cryptography-and-dual-watermarking-lsbdct-for-data-security/190852?camid=4v1a

DRM Practices in the E-Publication Industry
www.igi-global.com/chapter/drm-practices-publication-industry/13467?camid=4v1a