Chapter VII

Thoughts for the Future

Objectives of This Chapter

✓ Briefly put the previous information presented into a context for taking action.
✓ Understand the relationship between user privacy and data usage.
✓ Be aware of the relationship between security design and user features.
✓ Present some of the major issues in securing the global information infrastructure.
✓ Identify seven solutions for safeguarding the global information infrastructure from cyber criminals and cyber terrorists alike.
Introduction

In the previous chapters of this book, an examination of many of the approaches and motivations of terrorist organizations were presented, as well as their increasing use of the global information infrastructure to communicate, coordinate, and facilitate terrorist activities. The emergence of a cyber terrorist facilitating physical acts of violence in order to create widespread fear, brings with it a host of implications about the future of our electronic security. The vulnerabilities that continue to exist throughout telecommunication systems such as telephones, mobile accesses, cable, satellite, and Internet systems is blood in the water for hungry sharks of all kinds. Sectors such as public and private utilities, banking and finance, transportation, manufacturing, medical, education, and government, all use the global information infrastructure for daily operations and as such, may fall victim to these same technologies. It does not matter that the predator is a cracker, cyber criminal, or cyberterrorist when it comes to addressing corrective measures, or the underlying conditions and inherent dependencies that exist in today’s global environment. Because securing the global information infrastructure involves so many stakeholders, encompassing national and international interests that are governed by individual governments throughout the world, an examination of the larger political and economic issues must be discussed in order to construct preventive, corrective, and responsive initiatives.

In a 1995 paper by Ølnes and Spilling entitled *The new European regulatory environment for telecommunications – Implications for service management and its security*, the authors offer that market-driven nation states and economic federations are governed and impacted by the following:

- **General laws.** In any new initiatives, all relevant law, trade legislation, and treaties must be followed. This includes addressing the influences that can be asserted by the regulators such as the legislature and law enforcement.

- **National security and public order.** Because the integrity and availability of a country’s telecommunication infrastructure can be of critical importance, initiatives that change or alter these systems’ state of readiness will require direct input from those agencies responsible for maintaining national security and public order. This also includes the application of strong encryption when the monitoring of communications traffic is enacted in the name of national security.