IT Security Policy in Public Organizations

Parviz Partow-Navid
California State University, Los Angeles, USA

Ludwig Slusky
California State University, Los Angeles, USA

INTRODUCTION

Today, information security is one of the highest priorities on the IT agenda. In 2003, Luftman and McLean (2004) conducted a survey of Society for Information Management members to identify the top 20 information technology (IT) issues for executives. Security and privacy issues were ranked third, after IT/ business alignment and IT strategic planning. Concept of information security applies to all the data stored in information systems or being communicated in information networks and encompasses measures applied on all layers of open system interconnect (OSI) model of international standards such as application, networking, and physical.

Sophisticated technologies and methods have been developed to:

- Control access to computer networks
- Secure information systems with advanced cryptography and security models
- Establish standards for operating systems with focus on confidentiality
- Communication integrity and availability for securing different types of networks
- Manage trustworthy networks and support business continuity planning, disaster recovery, and auditing

The most widely recognized standards are:

- **In the United States:** Trusted Computer System Evaluation Criteria (TCSEC).
- **In Canada:** Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).
- **In Europe:** Information Technology Security Evaluation Criteria (ITSEC).

All of theses standards have recently been aggregated into Common Criteria standards. And yet, the information systems continue to be penetrated internally and externally at a high rate by malicious code, attacks leading to loss of processing capability (like distributed denial-of-service attack), impersonation and session hijacking (like man-in-the-middle attack), sniffing, illegal data mining, spying, and others. The problem points to three areas: technology, law, and IT administration.

Even prior to the drama of 9/11, several computer laws were enacted in the USA and yet more may come in the future. Still the fundamental threats to information security, whether they originated outside the network or by the company's insiders, are based on fundamental vulnerabilities inherent to the most common communication protocols, operating systems, hardware, application systems, and operational procedures. Among all technologies, the Internet, which originally was created for communication where trust was not a characteristic, presents the greatest source of vulnerabilities for public information systems infrastructures. Here, a *threat* is a probable activity, which, if realized, can cause damage to a system or create a loss of confidentiality, integrity, or availability of data. Consequently, *vulnerability* is a weakness in a system that can be exploited by a threat.

Although, some of these attacks may ultimately lead to an organization's financial disaster, an all-out defense against these threats may not be economically feasible. The defense actions must be focused and measured to correspond to risk assessment analysis provided by the business and IT management. That puts IT management at the helm of the information security strategy in public organizations.

INFORMATION SECURITY THREATS

Security threats to a computer system fall into a number of classes. Some well-known *threats* focus on disclosure of sensitive information; destruction of resources, interruption of processing, damage of data confidentiality, integrity, and availability, corruption, modification, theft, removal, and accidental loss, operator input error, and transaction processing errors.

Some threats influence the availability and reliability of the site, which is usually called a denial of service (DoS) attack. The Code Red virus is an example of a DoS attack.

Code Red was programmed to overflow Web servers with data, which it did so effectively that it resulted in making a huge portion of the Internet unavailable, as sites became clogged with more data than they could process. Other attacks target the content and data of a site, as individuals seek to damage, spy, steal, change, delete, or place something on the Web site. In addition, we have to be ready to deal with natural disasters such as earthquake, flood, and fire.

The common *purposes of the intended threats* include embezzlement and financial gains, curiosity, economic espionage, economic damage, personal financial injury, illegal search for evidence, and others.

The intruders employ a wide range of tools and techniques (some of them available on the Internet). A somewhat extensive but still incomplete list of hacker's tools and techniques include (Anderson, 2001; Preetham, 2002):

- **Backdoors:** Programs that are written to infect the victim's computer and open a secret door for the hacker.
- **Denial of Service (DoS):** Programs that designed to disrupt communications, sessions, transactions, or any other kind of business activities over the network.
- **Dumping Diving:** It is a process in which a social engineer searches an organization's garbage to find valuable information.
- Reading data erroneously left on the disk.
- **Impersonation:** In this approach, a social engineer gains detail information about an employee in an organization. Then the social engineer impersonates that employee by calling the help desk or another employee to gain access to sensitive information.
- **Loss of Processing Capability**
- **Man-in-the-Middle Attacks:** An attack in which a hacker can read, insert, and modify messages between two persons/systems without either one knowing that the communication line between them has been compromised.
- **Password Cracking:** Programs written to recover passwords from data that has been stored in or transmitted by a computer system, usually, by repeatedly verifying guesses for the password.
- **Replay Attack:** A form of nework attack in which a valid communiation is maliciously repeated or delayed. This is done by an attacker who intercepts the data and retransmits it as part of a masquerade attack.
- **Sniffers:** Programs that can see the traffic going throuhg a network or part of a network.
- **Social Engineering:** The greatest single danger identified by Information Security specialists (can be particularly damaging in public organizations)
- **Spoofing:** A technique hackers employ to alter the sender's identity within a packet.
- **Trojans:** Programs that provide a perceived benefit for the victim while conduction malicious activities in the background.
- **Viruses:** Programs that are written to crash a system, consume system's resources, or transmit vital information back to the hacker.
- **Worms:** Programs that are developed to replicate themselves on a desired medium. They are an effective tool for denial of service (DoS) attacks.

There are some preventive, detective, or response defense mechanisms, but each of them is effective only to some extent. None of them is full proof, and not all of them are economically or organizationally feasible for implementation at a public organization.

The list of hacker's tools and techniques is growing as new software (operating systems, applications, common-use utilities, and file types) continue to be introduced in the organizational and personal information networks. Information Security professionals agree that these trends will continue for foreseeable future.

COMPUTER LAWS

IT Security in public organizations must be guided by several computer laws which were enacted in the USA and which directly address specific issues of computer information privacy and protection:

- **Privacy Act of 1974:** To regulate federal government's use of private data.
- **Medical Computer Crime Act of 1984:** Sets federal criminal penalties for mi-use of medical records over telecommunications lines.
- **Comprehensive Crime Control Act of 1984:** Covered a range of computer crimes.
- **Computer Fraud & Abuse Act of 1986:** Defined computer fraud against federal interest computers.
- **Electronic Communications Privacy Act of 1986:** Covered illegality of capturing, altering or misuse of digital information.
- **Computer Security Act of 1987:** Defined security classification of electronic data.
- **Federal Sentencing Guidelines 1991:** Requires corporations to report computer crimes.
- **Economic Espionage Act of 1996:** Defined espionage against private companies.
- **U.S. National Information Infrastructure Protection Act of 1996:** Directly addresses the security of information systems and the need to protect the confidentiality, integrity and availability of information.