

Chapter 2



LEGAL ENVIRONMENT AND ITS IMPACT ON INFORMATION TECHNOLOGY

Introduction



Since the early 1970s, a number of laws have been passed and implemented within the US that deal with issues such as computer fraud and abuse, privacy, and security.

IT Crime Issues



- Computer crime costs organizations and individuals time and money
- Fewer than 10% of computer crimes are reported
- Categories of computer crime:
 - Computer is the target
 - Unauthorized access
 - Computer used to commit crime

Other Crimes



- Software piracy is an \$11 billion-dollar-a-year problem and rising
- Information Theft and Identity Fraud cases reported are increasing (Federal Trade Commission)
- Individual and consumer privacy violations (FTC)
- Electronic-commerce fraud

US Laws to Combat IT Crime



- Computer Fraud and Abuse Act of 1984, 1987 and 1994
 - Penalties include fines and/or imprisonment
 - Cover acts of
 - ✦ Fraudulent trespass
 - ✦ Intentional destructive trespass
 - ✦ Reckless destructive trespass

US Laws to Combat IT Crime



- Sarbanes-Oxley Act (PL 107-204)
 - Importance of due professional care and financial integrity
 - Cover acts of
 - ✦ Financial Fraud
 - ✦ Intentional destruction of records
 - ✦ Penalizes Executives for Non-Performance
 - Penalties include fines and/or imprisonment

Acts of Illegal Copying



- The U.S. Copyright Act of 1976, 1980
- The U.S. Mask Act
- The U.S. Patent Act
- The U.S. Federal Trademark Dilution Act of 1996
- Berne Convention

US Computer Security Act



- Passed in 1987
- Established a federal computer-security program
- NIST to assist in developing government wide, computer-system-security standards, guidelines, and security training

Homeland Security Act



- Passed in 2002
- Act demands life sentences for those hackers that "recklessly" endanger lives
- Act included provisions which seek to allow Net surveillance to gather telephone numbers, IP addresses, and URLs or e-mail information without recourse to a court

Homeland Security Act



- Internet Service Providers (ISPs) are required to hand users' records over to law enforcement authorities, overturning current legislation that outlaws such behavior
- The Homeland Security Act of 2002 was created to prevent terrorist attacks within the United States and reduce the vulnerability of the U.S to terrorism

Privacy Legislation



- The U.S. Privacy Act of 1974
- Electronic Communications Privacy Act of 1986 (U.S.)
- Communications Decency Act of 1995
- Children's Online Privacy Protection Act of 2000, 2008
- Encrypted Communications Privacy Act of 1996

Privacy Legislation (Cont)



- Health Insurance Portability and Accountability Act (HIPAA) 1996
- Risk Assessment and Communications Act of 1997
- Risk Gram-Leach-Bliley Act of 1999
- US Patriot Act of 2001
- Global activities in this area: Germany, France, China, Japan, etc.

Chapter Summary



- The legal environment of information systems is one the IT auditor cannot ignore and must keep pace with
- Within the U.S., new laws are being created and existing ones amended to reflect information technology's impact on us as individuals and as business entities

Class Exercise



- What products or studies or guidance has NIST issued in the last 5 years to help IT Auditors, IT Security Specialist and Management?
- In the agreement you signed with HR it indicates their use of ECPA to monitor your use of computer resources? Any use other than for business purposes may mean termination? What does this mean?