Chapter 3
Computer Crime, Ethics, and Privacy

• Introduction
• Computer Crime and Computer Abuse: An Overview
• Examples of Computer Crime Cases
• Thwarting Computer Crime and Abuse
• Computers and Ethical Behavior
• Computers and Privacy Issues

Computer Crime

• Computer crime
  – using the computer in a criminal act
  – either directly or indirectly
• Definition of computer crime is important
  – it affects how the statistics are accumulated.
• It is speculated
  – relatively small proportion of computer crime gets detected
  – and an even smaller proportion gets reported.

Computer Crime & Abuse: What’s the Difference?

• Computer crime
  – manipulation of a computer or computer data, by whatever method, to dishonestly obtain money, property or some other advantage of a value or to cause a loss.
• Computer abuse
  – the unauthorized use of, or access to, a computer for purposes contrary to the wishes of the owner of the computer.

Federal Legislation Affecting the Use of Computers

• Fair Credit Reporting Act of 1970
• Freedom of Information Act of 1970
• Federal Privacy Act of 1974
• Small Business Computer Security and Education Act of 1984
• Computer Fraud and Abuse Act of 1986
• Computer Fraud and Abuse Act (1996 amendment)
• Computer Security Act of 1987
• USA Patriot Act of 2001
• Cyber Security Enhancement Act of 2002
• CAN-SPAM Act of 2003

Legislation

• The Computer Fraud and Abuse Act of 1986 was perhaps the most important Federal legislation.
• Not be powerful enough to prosecute computer abuses of the 21st century such as types of Internet and telecommunications frauds.
Current initiatives

- Patriot Act renewal
- Internet Safety and Child Protection Act
- Internet Police Protection Act
- Anti-phishing Act

Privacy

- Gramm-Leach Bliley Act of 1999
- Credit card industry initiatives
- Fair and Accurate Credit Transactions Act of 2003

Kinds of Computer Crime

- Use of or the conspiracy to use computer resources to commit a felony
- Unauthorized theft, use, access modification, copying, or destruction of software or data
- Theft of money by altering computer records or the theft of computer time
- Theft, vandalism or destruction of computer hardware
- Intent to illegally obtain information or tangible property through the use of computers
- Trafficking in passwords or other login information for accessing a computer
- Extortion that uses a computer system as a target

Computer Fraud

- Computer fraud is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution.
- Economic espionage, the theft of information and intellectual property, is one type of computer fraud.

The Lack of Computer-Crime Statistics

- Good statistics on computer crime are mostly unavailable.
- Three reasons why statistics are unavailable are:
  1. private companies handle abuse internally
  2. surveys of computer abuse are often ambiguous
  3. most computer abuse is probably not discovered.

The Growth of Computer Crime

- Computer crime is growing because of
  - Exponential growth in computer resources
  - Internet pages give step-by-step instructions on how to perpetrate computer crime
  - Spending on computer controls has grown at a slow rate
Three Representative Computer Crimes Cases

- Compromising Valuable Information: The TRW Credit Data Case
- Computer Hacking: The Kevin D. Mitnick Case
- Denial of service: The 2003 Internet Crash
  - Through computer viruses
  - Through computer worms

The TRW Credit Data Case

- This valuable information computer crime is well known.
- The valuable information was computerized credit data.
- Two key issues:
  - the propriety of the input information
  - the protection afforded both consumer and user in the accuracy and use of credit information

The Kevin D. Mitnick Case

- Hackers are people who break into the computer files of others for fun or personal gain.
- Shoulder surfing is stealing calling credit numbers at public phones.
- Password controls can limit computer access to bona fide users.
- Social engineering is posing as bona fide employees.
- Lock-out systems disconnect telephone users after a set number of unsuccessful login attempts.
- Dial-back systems first disconnect all login users, but reconnect legitimate users after checking their passwords against lists of bona fide user codes.

Robert T. Morris and the Internet Virus

- Created one of the world’s most famous compute viruses.
- Became first person to be indicted under the Computer Fraud and Abuse Act of 1986.
- This case illustrates vulnerability of networks to virus infections.

Computer Viruses

- A computer virus is a program that disrupts normal data processing and that can usually replicate itself onto other files, computer systems or networks.
- Boot-sector viruses hide in the boot sectors of a disk, where the operating system accesses them.
- Worm viruses replicate themselves until the user runs out of memory or disk space.

Robert T. Morris and the Internet Virus Case

- Trojan Horse programs reside in legitimate copies of computer programs.
- Logic Bomb programs remain dormant until the computer system encounters a specific condition.
- A virus may be stored in an applet, which is a small program stored on a WWW server.
Methods for Thwarting Computer Viruses: Anti-Virus Software

- **Anti-virus software** includes computer programs that can:
  - scan computer disks for virus-like coding;
  - identify active viruses already lodged in computer systems;
  - cleanse computer systems already infected;
  - perform a combination of these activities.

Drawbacks of Anti-Virus Software Programs

- Anti-virus programs provide less-than-complete protection because
  - new, more powerful viruses are always being written that can avoid known detection schemes.
  - anti-virus programs can contain virus routines.

Anti-Virus Procedural Controls

- Buy shrink-wrapped software from reputable sources
- Avoid illegal software copying
- Do not download suspicious Internet files
- Do not open email messages from unknown sources - Delete them
- Maintain complete backup files
- Keep email, office and operating systems updated

Organizational Safeguards Against Computer Viruses

- Educate employees about viruses.
- Encourage employees to follow virus prevention and detection techniques.
- Establish policies that discourage the free exchange of computer disks or externally acquired computer programs.
- Use computer passwords to thwart unauthorized users from accessing the company's operating systems and files.
- Use anti-virus filters on LANs and WANs.
- Have an approved and tested disaster recovery plan.

Methods for Thwarting Computer Abuse

- Enlist top management support
- Increase employee awareness and education
- Conduct Security Inventory and protect passwords
- Implement controls
- Identify computer criminals
  - Look at technical backgrounds, morals, and gender and age

Methods for Thwarting Computer Abuse

- Recognize the symptoms of employee fraud
  - Accounting irregularities such as forged, altered or destroyed input documents
  - Internal control weaknesses
  - Behavioral or lifestyle changes in an employee
  - Unreasonable anomalies that go unchallenged
- Employ forensic accountants

Employ forensic accountants
Computers and Ethical Behavior

- **Ethics** is a set of moral principles or values.
- **Ethical behavior** involves making choices and judgments that are morally proper and then acting accordingly.
- Ethics can govern and organization as well as individuals.

Ethical Issues

- Honesty
- Protecting Computer Systems
- Protecting Confidential Information
- Social Responsibility
- Rights of Privacy
- Acceptable Use of Computer Hardware and Software.

How Organizations Encourage Ethical Behavior

- Inform employees that ethics are important.
- Formally expose employees to relevant cases that teach how to act in specific situations.
- Teach by example, that is, by managers acting responsibly.
- Use job promotions and other benefits to reward those employees who act responsibly.
- Encourage employees to join professional organizations with codes of conduct such as Codes of Conduct and Good Practice for Certified Computer Professional.

Computers and Privacy Issues

- Company policies with respect to privacy
  - Privacy policy
  - Disposal of computers
- Online privacy seals

Copyright

Copyright 2005 John Wiley & Sons, Inc. All rights reserved. Reproduction or translation of this work beyond that permitted in Section 117 of the 1976 United States Copyright Act without the express written permission of the copyright owner is unlawful. Request for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.