CYBER CRIMES

Objective

During this session, participants will examine cyber crime offenses and other offenses related to computers and the Internet.

I. WHAT IS "CYBER CRIME"?

A. Cyber crimes

1. Offenses against computer data and systems
2. Offenses related to computers and the Internet
3. Computers are essential to the crime
4. Other crimes may create digital evidence

B. International standards provide a framework for discussing cyber crime

1. Cyber crime is a worldwide challenge, but ***domestic*** laws establish cyber crime offenses
2. As governments, commerce, and people rely more on computers and the Internet, countries must continue to improve their cyber crime laws; this is necessary to enable successful investigation and prosecution, and improve international legal cooperation
3. The ***Convention on Cybercrime*** provides a framework for discussing cyber crime law, including:
    a. Crimes related to computers and the Internet
    b. Provisions for investigating cyber crime
    c. International legal cooperation
    d. Protection of human rights and liberties
4. This Council of Europe treaty entered into force in January 2004, and is open to all countries in the world; as of January 2008, 22 countries are parties, another 21 countries have signed but are not yet parties, and other countries are interested in joining; the convention and additional materials are at http://conventions.coe.int/

C. Important definitions

1. Computer system: Any device consisting of hardware and software developed for automatic processing of digital data; it may stand-alone or part of a network; a computer system usually consists of different devices, including a processor and peripheral
2. Network: An interconnection between two or more computer systems; data is exchanged over the network

3. Computer data: Any representation of facts, information, or concepts in a form suitable for processing in a computer system; this includes electronic and digital information and programs

II. OFFENSES AGAINST COMPUTER DATA AND SYSTEMS

A. Illegal access: When committed intentionally, the access to the whole or any part of a computer system without right; often referred to as "hacking", "cracking", or "computer trespass"; illegal access may result in damage to computer systems and data or compromise of confidential data (Convention, Article 2)

B. Illegal interception: When committed intentionally, the interception without right, made by technical means, of non-public transmission of computer data to, from, or within a computer system; seeks to protect the privacy of non-public computer data transmissions from monitoring and recording (Convention, Article 3)

C. Data interference: When committed intentionally, the damaging, deleting, deterioration, alteration, or suppression of computer data without right; includes inputting of malicious codes (for example, viruses) that can threaten the integrity or use of data or programs (Convention, Article 4)

D. System interference: When committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data; includes inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (for example, denial of service attacks and viruses that stop or slow computer systems) (Convention, Article 5)

E. Misuse of devices: When committed intentionally and without right, the production, sale, procurement for use, import, distribution, or otherwise making available of:

1. Access devices, including computer programs,
2. Computer passwords, codes, or other access data,

for the purpose of committing a cyber crime; access devices with a legitimate use are generally not contraband unless the ***primary*** purpose is illegal (Convention, Article 6)

III. OFFENSES RELATED TO COMPUTERS AND THE INTERNET

A. Computer-related forgery: When committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic; may require an intent to defraud (Convention, Article 7)

B. Computer-related fraud: When committed intentionally and without right, causing a loss of property to another person by:

1. Any input, alteration, deletion, or suppression of computer data,
2. Any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself of another person; includes economic crimes such as online credit card fraud (Convention, Article 8)

C. Child pornography: When committed intentionally and without right, the following conduct:

1. Producing child pornography for the purpose of its distribution through a computer system
2. Offering or making available child pornography through a computer system
3. Distributing or transmitting child pornography through a computer system
4. Procuring child pornography through a computer system for oneself or for another person
5. Possessing child pornography in a computer system or on a computer data storage medium

(Convention, Article 9)

D. Intellectual property infringement: Willful infringement of copyright and related rights on a commercial scale and by means of a computer system (Convention, Article 10)

E. Ancillary liability (Convention, Articles 11-12)

1. Attempt and aiding or abetting
2. Corporate liability, the liability of "legal persons"

This presentation was developed by the Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, www.cybercrime.gov