CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

# Security Auditing, Legal and Ethical Aspects

## Cybercrime

# Video Summary

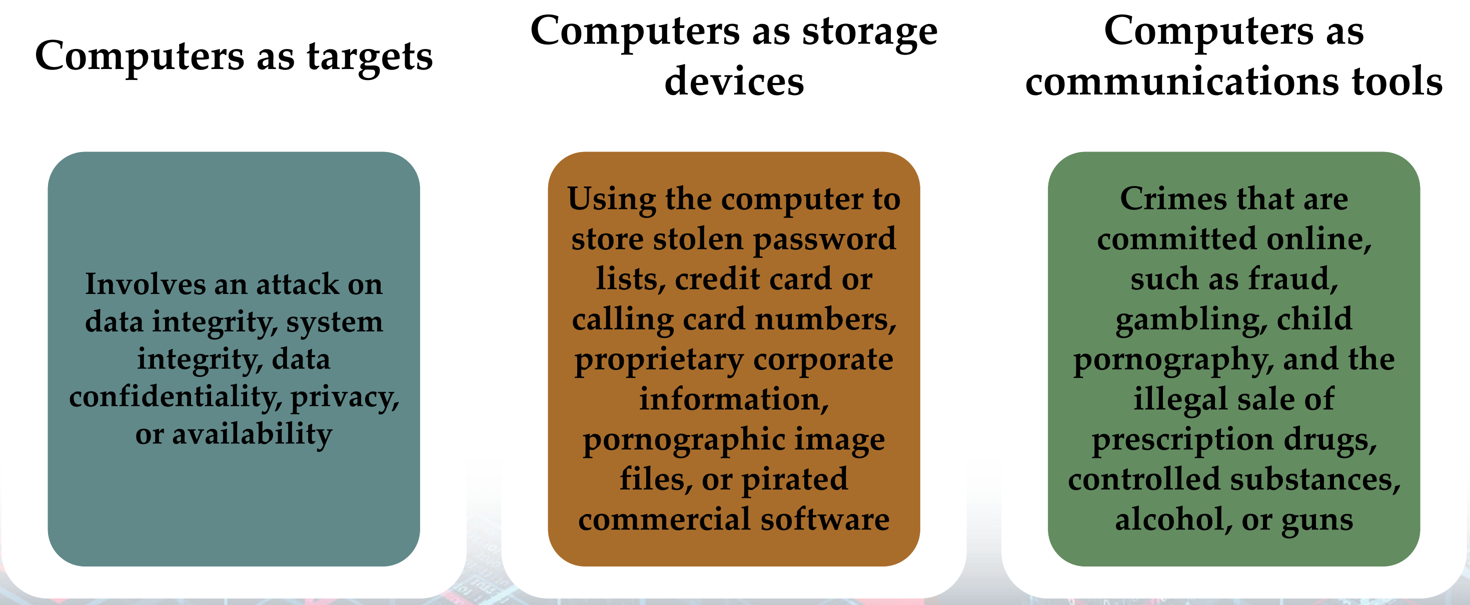
- What is A Computer Crime or Cybercrime?
- Types of Computer Crime
- Law Enforcement Challenges
- Cybercriminals
- Cybercrime Victims

“Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.”

*--From the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement*

# Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:



**Computers as targets**

Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

**Computers as storage devices**

Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

**Computers as communications tools**

Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

# Cybercrimes Cited in the Convention on Cybercrime

**Article 2 Illegal access**

The access to the whole or any part of a computer system without right.

**Article 3 Illegal interception**

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

**Article 4 Data interference**

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

**Article 5 System interference**

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

**Article 6 Misuse of devices**

- **a** The production, sale, procurement for use, import, distribution or otherwise making available of:
  - **i** A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
  - **ii** A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and
- **b** The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

**Article 7 Computer-related forgery**

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, regardless whether or not the data is directly readable and intelligible.

**Article 8 Computer-related fraud**

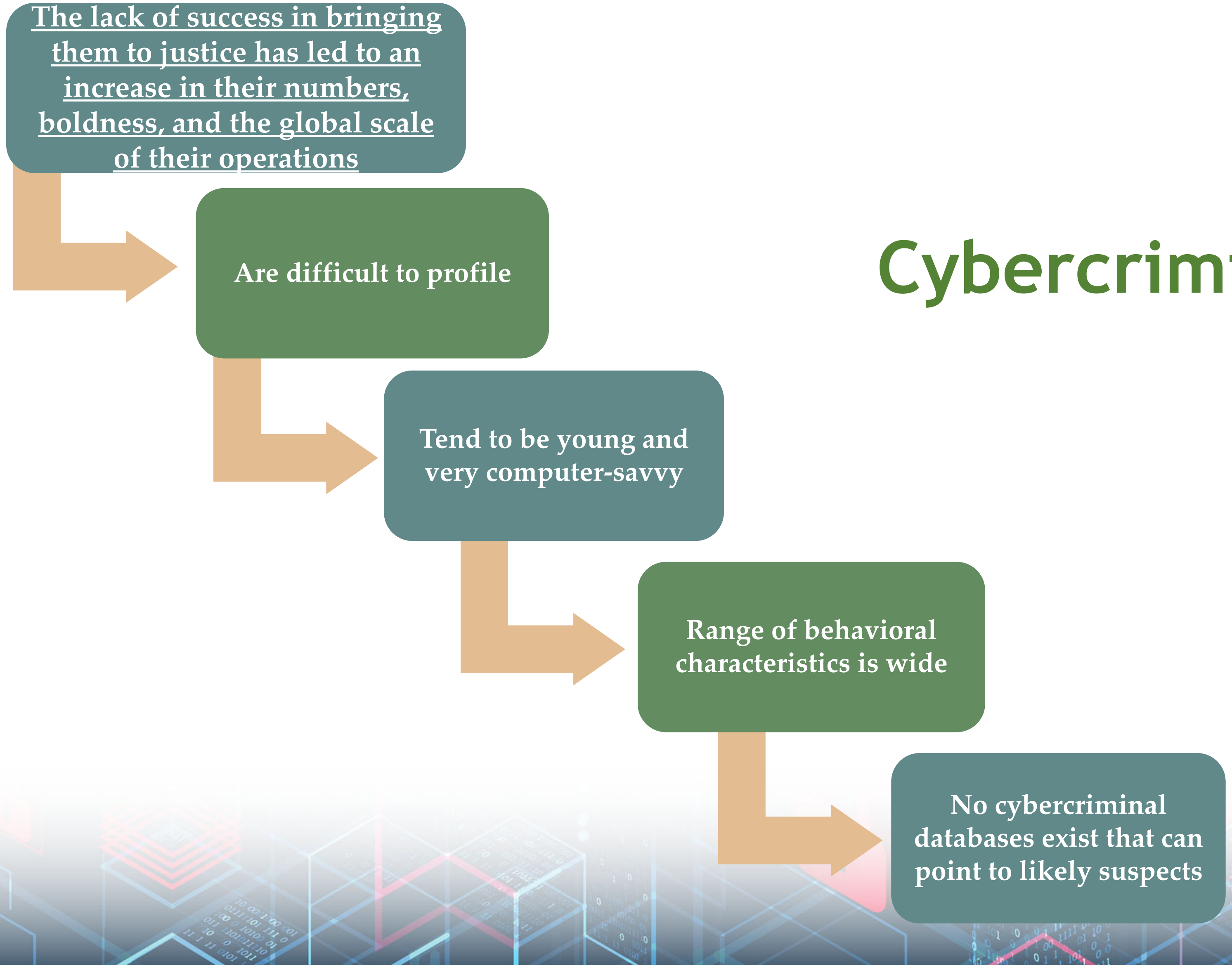
The causing of a loss of property to another person by:

- **a** Any input, alteration, deletion or suppression of computer data;
- **b** Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

# Law Enforcement Challenges

- Law enforcement agency difficulties:
  - Lack of investigators knowledgeable and experienced in dealing with this kind of crime
  - Required technology may be beyond their budget
  - The global nature of cybercrime (the criminal is in another country)
  - Lack of collaboration and cooperation with remote law enforcement agencies

# Cybercriminals



The lack of success in bringing them to justice has led to an increase in their numbers, boldness, and the global scale of their operations

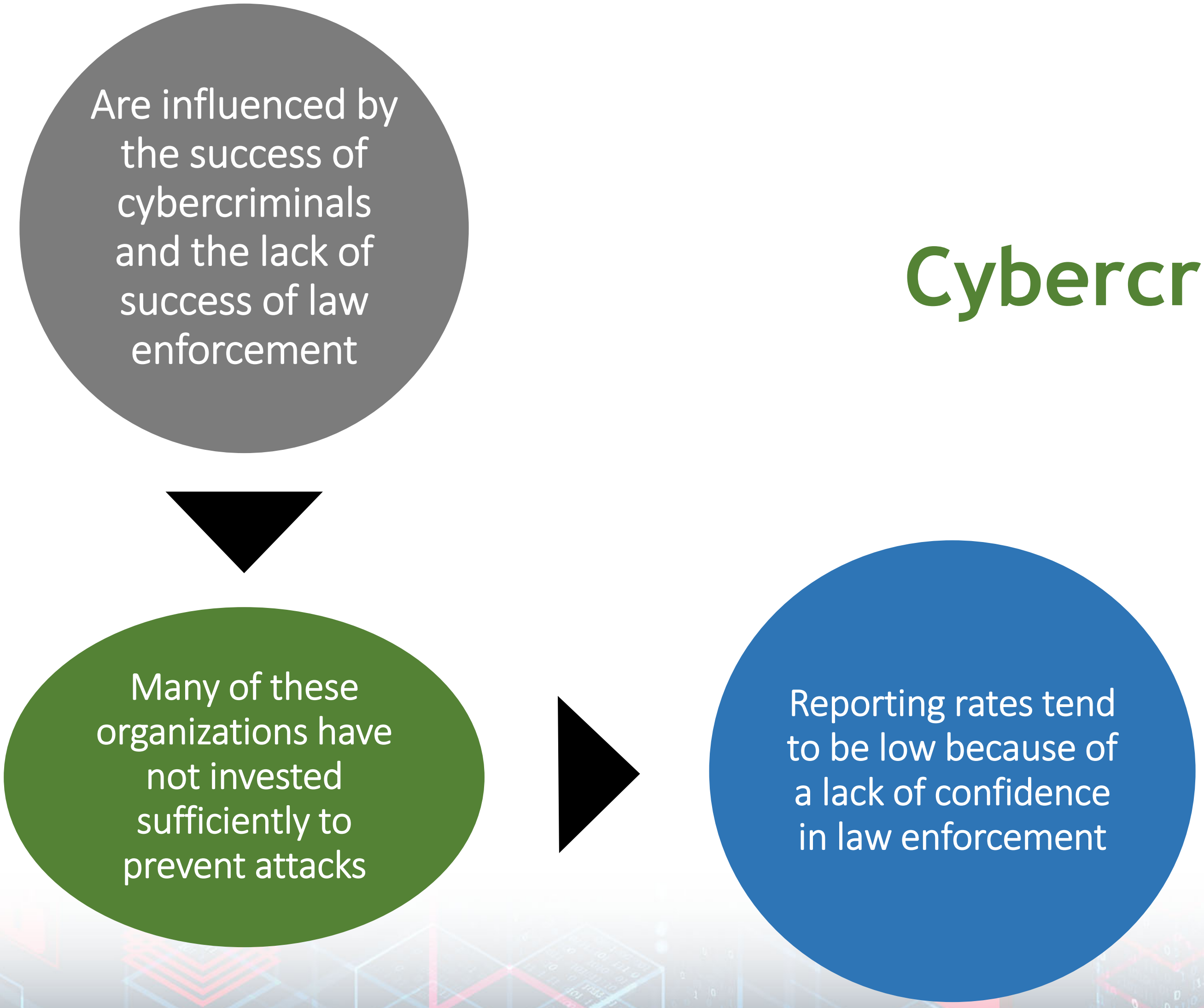
Are difficult to profile

Tend to be young and very computer-savvy

Range of behavioral characteristics is wide

No cybercriminal databases exist that can point to likely suspects

# Cybercrime Victims



Are influenced by the success of cybercriminals and the lack of success of law enforcement

Many of these organizations have not invested sufficiently to prevent attacks

Reporting rates tend to be low because of a lack of confidence in law enforcement

# Working with Law Enforcement

- Executive management and security administrators need to look upon law enforcement as a resource and tool

- Management needs to:
  - Understand the criminal investigation process
  - Understand the inputs that investigators need
  - Understand the ways in which the victim can contribute positively to the investigation

# Video Summary

- What is A Computer Crime or Cybercrime?
- Types of Computer Crime
- Law Enforcement Challenges
- Cybercriminals
- Cybercrime Victims