

Course Learning Outcomes for Unit III

Upon completion of this unit, students should be able to:

1. Explain how criminal justice theories and technologies impact the commission and solution of crime.
 - 1.1 Define the various cybercrimes and threats.
 - 1.2 Explain the various criminal organizations prevalent in cybercrime.
2. Evaluate criminal justice strategies, policies, and procedures to determine best practices.

Reading Assignment

Chapter 5: Sophisticated Cyber Criminal Organizations

Chapter 6: White-Collar Crimes

Unit Lesson

There is something very James Bond about this unit: espionage, covert organizations, and rogue former employees. One can almost see the remote and deserted island with the evil genius mastermind and his room full of servers that can infiltrate any system with the touch of a button. Fiction? Maybe, maybe not.

Moving away from the discussion of hackers, there are much more sophisticated cybercriminals. You can keep your image of the little guy sitting in his parents' basement as your cybercriminal, if you wish. Hey, he may work for the big guys.

Who are the big guys? They are everywhere. If you chose to believe in La Cosa Nostra, they are a threat. Remember, successful enterprises, legal or not, are always on the cutting edge of technology and opportunity. When you think of money laundering, you might automatically think about organized crime (e.g., the mob or Tony Montana with all of his "businesses"). Nowadays, organized crime has a way to launder their money in a more efficient and clandestine way: through technology.

There are multiple criminal organizations that cover almost every region in the world: African, Russian, Italian, and Asian, among others. The threat of cybercrimes on this global scale calls into question several issues of international law. What law applies? Who can bring charges? What happens when a non-cooperative government is involved? Are some of these crimes un-prosecutable?

There are other sophisticated criminals to whom the term *organized crime* does not apply. These are your white collar criminals. These are trusted advisors, employees, and other fiduciaries that use their position for their own financial gain, and ultimately, the company's downfall. This is where one must distinguish between using computers to facilitate the crime and using malware or viruses to commit the crime. For a very rudimentary example, think about the movie *Office Space*. These three yahoos used a computer program to siphon off small percentages of money they deemed too small to be traceable and wound up with hundreds of thousands of dollars almost overnight.

Computer Crimes

Click on the following link to view an interactive presentation about computer crimes:

<http://www.pearsoncustom.com/mct-enterprise/asset.php?isbn=1256689785&id=15772>

Internet-Based Crimes

Click on the following link to view an interactive presentation about internet-based crimes:

<http://www.pearsoncustom.com/mct-enterprise/asset.php?isbn=1256689785&id=15771>

How can we not mention Bernie Madoff? He is a white collar criminal who embezzled millions of dollars. In fact, he is deemed to have committed the largest financial fraud in U.S. history. He did this using computers and inputting fraudulent information. You are encouraged to do some independent research on this case. Many of you may have heard about him, but it is important to understand the facts and details of any case, beyond the media reports. Not only does the media not always report everything, for reasons of time, politics, and interest, the meat of the story and how it was done is so much more interesting than a basic headline, not to mention horrifying, and horrifyingly simple. In the next unit you will take a look at how these cybercriminals operate.

Suggested Reading

Chapter 5 PowerPoint: Sophisticated Cyber Criminal Organizations

Click [here](#) for a PDF version of the Chapter 5 Presentation.

Chapter 6 PowerPoint: White-Collar Crimes

Click [here](#) for a PDF version of the Chapter 6 Presentation.

Course Learning Outcomes for Unit IV

Upon completion of this unit, students should be able to:

3. Analyze research methodologies, training, and development techniques that result in effective management of criminal justice programs.
 - 3.1 Identify the technical facets of cybercrime for identification and management of crime.
 - 3.2 Identify the history and identification methods of cybercriminals for identification and management of crime.

Reading Assignment

Chapter 7: Viruses and Malicious Code

Unit Lesson

We have talked about the criminals: the greasy kid in his parents' basement, the sleek James Bond villain, and everyone in between. Now, it is time to get to the nuts and bolts of what they do and how. This is where a lot of people's brains are going to short circuit...pun intended. There is going to be a lot of talk and learning about the technical aspects of these crimes. Stay with it here though because it is important to understand what people are doing in order to properly identify the specific illegal activity, catch the perpetrator, and prosecute under the relevant law, if applicable.

To put a less dry spin on it, think about the psyche of the criminals. Remember back to our lesson on criminal justice theories. For the same reasons we cannot pigeon hole every criminal into the same theory or psychological condition, we cannot think of all cybercrimes and the methods by which they are committed as the same.

As with violent criminals, there are different types of cybercriminals. Some want their genius to be known, or they want to be caught, or at least, they think it is fun playing cat and mouse with the authorities and the public. Check out the movie *Copycat*, and match that criminal with the BTK killer and the Zodiac killer. They all taunted the police. Contrast this type of criminal with Ted Bundy or Charles Manson. They did not want to be caught. Certainly, Bernie Madoff did not want to be caught. As you look at these crimes and these criminals, it is important to understand how they do what they do in order to track them down or beat them at their own game.

The methodologies of these crimes are a very important piece of the puzzle for a law enforcement officer. Sure, not all members of the criminal justice team (the arresting officer for example) need to know how *basement boy* committed the crime, but the detective and the prosecutor must know.

Does this mean you must become an expert on malware and stay up with the latest viruses? Yes, it does, if your chosen path is identifying and detecting these crimes and their criminals. Otherwise, a solid foundation will suffice. This leads into the part of the unit where you will look at the different types of codes and viruses, worms, adware, and spyware.

Identifying the Tools of Cyber Terrorists

Click on the following link to view an interactive presentation about the tools of cyberterrorists:

<http://www.pearsoncustom.com/mct-enterprise/asset.php?isbn=1256689785&id=16060>

Surely you have heard of a Trojan horse virus, but can you define it? Do you remember the Melissa virus several years ago? How did that work? How come when you are on Google and Facebook, the ads match up with things you search for on your web browser? "Wait a minute," you say. "Those are ads. That is not a crime." That may be arguable, but it is an infiltration, and maybe just a few steps away from a criminal infiltration. In the next unit, you will learn about how it is done.

Suggested Reading

Chapter 7 PowerPoint: Viruses and Malicious Code

Click [here](#) for a PDF version of the Chapter 7 Presentation.