

## 1.3.4 Lab - Visualizing the Black Hats (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Research and analyze cyber security incidents.

### Background / Scenario

The FBI has estimated that cybercrime cost individuals and companies over 3.5 billion dollars in 2019. Governments, businesses, and individual users are increasingly the targets of cyberattacks and cybersecurity incidents are becoming more common.

In this lab, you will create three hypothetical cyber attackers, each with an organization, an attack, a motive. In addition, suggest a method by which an organization could prevent or mitigate the attack.

**Note:** You can use the web browser in the virtual machine that was installed in a previous lab to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

### Required Resources

- PC or mobile device with internet access and virtual machine (optional)

### Instructions

#### Scenario 1:

- a. Who is the attacker?

**Answers will vary.**

- b. What organization or group is the attacker associated with, if any?

**Answers will vary.**

- c. What is the motive of the attacker?

**Answers will vary.**

- d. What method of attack was used?

**Answers will vary.**

- e. What was the target and vulnerability used against the business?

**Answers will vary.**

- f. How could this attack be prevented or mitigated?

**Answers will vary.**

## Scenario 2:

- a. Who is the attacker?

**Answers will vary.**

- b. What organization/group is the attacker associated with?

**Answers will vary.**

- c. What is the motive of the attacker?

**Answers will vary.**

- d. What method of attack was used?

**Answers will vary.**

- e. What was the target and vulnerability used against the business?

**Answers will vary.**

- f. How could this attack be prevented or mitigated?

**Answers will vary.**

### Scenario 3:

- a. Who is the attacker?

**Answers will vary.**

- b. What organization/group is the attacker associated with?

**Answers will vary.**

- c. What is the motive of the attacker?

**Answers will vary.**

- d. What method of attack was used?

**Answers will vary.**

- e. What was the target and vulnerability used against the business?

**Answers will vary.**

- f. How could this attack be prevented or mitigated?

**Answers will vary.**