Cybersecurity Investigator 1

Briefing Cards

Briefing Card #1:

There has been a cyber attack on our city! At 7:48 a.m., we became aware of a ransomware attack on our city.

We are working with law enforcement to figure out who hacked into our city's networks. In the meantime, I ask that each individual department take inventory of the level of damage that your department has experienced. Please think through the implications of this attack. Most immediately, how will this attack affect citizens in our city? And how will it affect employees within your department?

In five minutes, we will reconvene for another briefing meeting. At that time, each department head will present a summary of the damages to her department. Thank you all for your help in this crisis.

Briefing Card #2:

There has been a break in the case!

Law enforcement officials believe that a known hacker network, called HaShTaG, was behind the attack. This group often communicates using steganography: that is, hiding messages in plain sight.

In the weeks leading up to the attack, there was an increase in chatter on online message boards about ransomware attacks. They have identified one thread in particular, to which they believe the HaShTaG hackers were contributing.

Until further notice, please give all of your attention to this thread and try to identify any users who you think might be affiliated with the HaShTaG hacker group.

Briefing Card #3:

As you all know, our city fell victim to a ransomware attack this morning. Ransomware is a type of malware that denies you access to your data until you pay a ransom. In all of the affected departments, computers are locked with a screen that contains a ransom request. The attackers are requesting that the city pay a Bitcoin ransom in order to regain access to our computers and data. We only have 20 minutes to make a decision. What do you think we should do?

Ask all of the department heads whether or not they think we should pay the ransom, and why. Give the department heads a chance to discuss and debate their ideas, knowing that you will be the one to make the final decision.

Briefing Card #4:

DECISION: PAY THE RANSOM

Your city has decided to pay the ransom in Bitcoin. However, when you went to pay the ransom, you found that the dark web communication portal between the attackers and the city had already been taken down! This means that, in spite of your best intentions, any opportunity to pay the ransom has officially closed, and there is no foreseeable way to retrieve your data directly from the hackers. You hire a cybersecurity company to try and recover as much data as possible without the encryption key. This company warns that recovery from this attack may cost a lot of money and take months to complete.

In the meantime, you must turn your attention to the following priorities:

- Identify which hacker (or hackers) carried out the attack
- Find out where and how the breach happened
- Put systems in place to try and prevent future attacks

Briefing Card #5:

DECISION: DO NOT PAY THE RANSOM

Your city has decided not to pay the ransom in Bitcoin. This means that that you will not be able to receive the encryption key from the hackers, which would unlock all of your data. You hire a cybersecurity company to try and recover as much data as possible without the encryption key. They warn that recovery from this attack may cost a lot of money and take months to complete.

In the meantime, you must turn your attention to the following priorities:

- Identify which hacker (or hackers) carried out the attack
- Find out where and how the breach happened
- Put systems in place to try and prevent future attacks