13.2.6 Solutions

1. *Types of Incidents* The correct matching of types of incident and description are shown in table 13.4.

Phishing	This type of incident typically uses email as its medium of attack. The malicious user sends an email pretending to be a legitimate sender and aims for the target to either click a malicious link or download a malicious file.
Ransomware	This type of incident typically involves locking the targets assets by encrypting their hard drive. The malicious user promises to unlock the targets assets upon receiving a sum of money.
Denial of Service	This type of incident typically involves flooding a targets asset with so much traffic that it is unable to operate properly. The malicious user sends a mass of network traffic to the target system until it crashes or is otherwise unable to perform its intended task.
Malware	This type of incident is categorized by malicious code or software. The malicious user crafts special code to compromise the security of the target system in hope to steal data or damage the target system.

Table 13.4: *Matching Incident Types to Descriptions*

2. *The Stages of Incident Response*

   A combination of the NIST and SANS incident response plans results in the following steps for incident response:

   (a) Prepare for an Incident

   (b) Identify and Analyze an Incident

   (c) Contain the Incident

   (d) Eradicate the Incident

   (e) Recover from the Incident

   (f) Perform an Analysis Post Incident

3. *Assess an Existing Incident Response Plan*

   This plans strengths are that it vaguely suggests that the organization should identify and

analyze the incident (detect the incident) and eradicate the incident (get rid of the threat). The terminology needs to be more concrete here. The step to involve law enforcement should not be on the list. Law enforcement should only be involved as necessary.

4. *Develop a New Incident Response Plan*

   Be sure to note the following items are noted and documented for each incident:

   - Date
   - Time
   - Detecting Individual
   - Systems Impacted
   - Description of Incident
   - Steps Taken in Response

   Incident #1

   Be sure to question whether or not personal devices should be connected to the same network as business assets. Your discussion should include a plan to hold phishing awareness training after the incident.

   Incident #2

   Be sure to question why customers are not connecting to a guest network instead of the business network. Your discussion should include conversation regarding whether or not the ransom should be paid. Also comment on what steps should be taken with doors opening in less than two hours from the detection of the incident.

   Incident #3

   Your discussion should include a plan to hold training on removable device hygiene. Also discuss what actions may need to be taken since loss of life is a potential consequence in this case.

5. *Brief Audiences on Incidents*

   Criteria which should be noted in the briefing include:

- Date
- Broadly, what systems are impacted
- Broadly, what the impact was
- In detail, what has been done so far in response
- In detail, the plan going forward

The briefing should begin with a brief description of the incident, then cover the criteria above, end the session with a question-answer period. Be sure not to give away any details which may be considered confidential according to your organizations classification program or any information which is too technical, the audience is likely more interested in what the incident means for them, what has been done to fix it, and how you can assure them it will not happen again.