Objective: This assessment is designed to evaluate students' understanding of the ransomware simulation, their problem-solving skills, and their ability to think critically about cybersecurity issues. The multiple-choice questions focus on factual recall, while the open-ended questions encourage deeper reflection and application of the concepts learned.

Multiple Choice Questions:

1. **What type of cyber threat did <<Enter School Name Here>> face in the simulation?**

   a) Phishing
   b) Ransomware
   c) Trojan Horse
   d) Virus

2. **What should be the first step in responding to a ransomware attack?**

   a) Pay the ransom
   b) Disconnect infected systems from the network
   c) Delete all files
   d) Announce the attack on social media

3. **Which team was responsible for managing internal and external communications?**

   a) IT Team
   b) Administration Team
   c) Communications Team
   d) Crisis Management Team

4. **What was one of the clues provided to identify the ransomware?**

   a) A note written in a foreign language
   b) A suspicious email in a staff member's inbox
   c) A random phone call
   d) A hidden message in a school announcement

5. **What role did the Crisis Management Team play in the simulation?**

   a) Organized the school prom
   b) Oversaw the overall response to the crisis
   c) Provided technical support
   d) Managed the school cafeteria

6. **What should be included in a recovery plan for a ransomware attack?**

   a) Steps for data and system restoration
   b) A party to celebrate

c) Plans for a school field trip
d) A new school mascot design

7. **Which of the following is not a typical vector for ransomware infection?**

   a) Phishing emails
   b) Using outdated software
   c) Downloading from untrusted sources
   d) Secure websites

8. **What action is crucial for mitigating the impact of a ransomware attack?**

   a) Updating social media statuses
   b) Regularly backing up data
   c) Changing the wallpaper on all computers
   d) Unplugging the coffee machine

9. **How should sensitive data leaks be handled in a ransomware situation?**

   a) Ignored
   b) Shared on social media
   c) Reported to relevant authorities and stakeholders
   d) Deleted immediately

10. **Why is regular cybersecurity training important for staff and students?**

    a) To fill up the school curriculum
    b) To keep them aware of evolving cyber threats
    c) To ensure they spend less time on social media
    d) To prepare them for IT careers

Open-Ended Questions

1. Describe the key steps your team would take immediately after discovering the ransomware attack.

   Possible responses may include:
   - **Isolate affected systems.**
   - **Alert the IT and Crisis Management Teams.**
   - **Secure backups and assess data loss.**
   - **Begin documentation and communication protocols.**

2. How would you approach the decision-making process regarding whether to pay the ransom or not?

   Possible responses may include:

- **Assess the impact and likelihood of data recovery.**
- **Consider legal and ethical implications.**
- **Evaluate the credibility of the threat.**
- **Consult with cybersecurity experts and law enforcement.**

3. Outline a basic recovery plan to restore systems and data following the ransomware attack.

   Possible responses may include:
   - **Restore data from backups.**
   - **Cleanse and secure the network.**
   - **Update and patch systems.**
   - **Review and enhance security protocols.**

4. Discuss the importance of cybersecurity awareness and training in preventing future ransomware attacks.

   Possible responses may include:
   - **Prevents potential breaches.**
   - **Builds a culture of security.**
   - **Helps in the early detection of threats.**
   - **Minimizes the impact of attacks.**

5. Reflect on the lessons learned from participating in the ransomware simulation and how they could be applied in real-life situations.

   Possible responses may include:
   - **The importance of preparedness and response plans.**
   - **The value of teamwork and clear communication.**
   - **Understanding the evolving nature of cyber threats.**
   - **The significance of regular updates and backups.**