Title: <<Enter Your School Name Here>>

Date: <<Insert Date>>

Background: <<Enter Your School Name Here>> computer network has been compromised in a calculated ransomware attack. Vital school records, student information, and administrative data have been encrypted by unknown attackers demanding a ransom.

Situation Overview:

- **Time of Attack Discovery:** 8:00 AM, Monday.
- **Initial Discovery:** The school's IT department noticed unusual network activity and inaccessible files across multiple systems.
- **Current Status:** Key systems are locked, including grade databases, staff payroll, and email servers. A ransom note has been received, demanding payment in cryptocurrency.

Ransom Note Details:

Demand: $50,000 in Bitcoin.
Deadline: 72 hours from the time of the attack discovery.
Threat: The attackers threaten to delete all data permanently if the ransom is not paid.

Operational Teams:

- **Information Technology (IT) Team:** Responsible for technical response, including identifying the malware, isolating infected systems, and exploring recovery options.
- **Administration Team:** Focused on decision-making regarding the ransom payment and coordinating with external authorities.
- **Communications Team:** In charge of internal and external communication, managing information released to staff, students, and media.
- **Crisis Management Team:** Overseeing the overall response, ensuring all teams work cohesively, and planning long-term recovery and prevention strategies.

Objectives:

Identify the Type of Ransomware: Analyze clues and data to determine the specific ransomware variant.

Formulate a Response Plan: Decide on immediate actions, including whether to pay the ransom or seek alternative solutions.

Develop a Recovery and Prevention Plan: Propose steps to restore systems and prevent future attacks.

Note to Participants: This simulation is designed to challenge your problem-solving, teamwork, and decision-making skills in a high-pressure scenario akin to real-world cyber threats. Your choices will impact the unfolding of the event, and there are no 'right' or 'wrong' decisions, only consequences to navigate.

Goood Luck Teams!

Your response to this crisis will test your ability to handle a real-world cybersecurity threat. Remember, communication and collaboration are key to a successful outcome.