Objective: These developments simulate real-world cybersecurity incidents' dynamic and often unpredictable nature, testing the student's ability to adapt to changing situations and make critical decisions under pressure.

Further Development in the Scenario

Development 1: Urgent Update

- **Time:** 24 hours after the initial discovery of the attack.
- **Event:** An anonymous tip is received, suggesting that the ransomware may have an internal source – possibly someone with access to the school's network.

Development 2: Unexpected Complication

- **Time:** 36 hours after the attack.
- **Event:** The school's backup systems, thought to be unaffected, are found to be corrupted as well, making data recovery more challenging.

Development 3: Media Involvement

- **Time:** 48 hours after the attack.
- **Event:** A local news outlet catches wind of the situation and broadcasts a story, putting additional public pressure on the school's response.

Development 4: Additional Threat

- **Time:** 55 hours after the attack.
- **Event:** A second ransom note is received, doubling the ransom amount and shortening the deadline, citing the media attention as a reason.

Development 5: External Assistance Offer

- **Time:** 60 hours after the attack.
- **Event:** A cybersecurity firm reaches out, offering assistance in decrypting the files but at a significant cost.

Development 6: Breakthrough Clue

- **Time:** 65 hours after the attack.
- **Event:** A hidden log file is discovered by the IT team, revealing a potential weakness in the ransomware's code.

Development 7: Ethical Dilemma

- **Time:** 68 hours after the attack.
- **Event:** A group of students confess to accidentally downloading the ransomware, fearing repercussions, they initially kept silent.

Development 8: Final Countdown

- **Time:** 70 hours after the attack.
- **Event:** The attackers send a final warning, with a more aggressive tone, threatening to leak sensitive data publicly if the ransom is not paid.