Update 1:

Grades for hire …

Review of the network and system logs indicates that the attackers logged in from the school’s Wi-Fi network after school hours.

Reports have surfaced at school about a couple of students offering to change additional grades for money. No names have yet been revealed.

Update 2:

An after school special …

Two juniors are rumored to be the culprits. Administrators call the students into the office to ask them about the rumors.

Students admit that they had found a sticky note with a teacher’s username and password, which they used to log in after school to change the grades.

They also admit that they accessed some other school systems, including an employee database that lists names, addresses, SSNs, employee ID numbers, etc.

Update 3:

It’s gone viral!

The data the students accessed contain sensitive personal information for {insert number} students and {insert number} employees.

Some of the staff’s personal data have been posted on the students’ Facebook pages and are now available on the Internet.

With all the attention and social network exposure, the news of the breach has leaked out. Parents are calling you asking if their child’s data were accessed and their grades changed.

Press Conference Time

News of the breach is out there, so now you must brief the press and the community.

Your spokesperson will give a brief press conference to address the issue and take questions.

The audience includes reporters from local and national media, as well as parents, privacy advocates, and activists.

Develop Incident Response Plan

Use your notes from the scenario discussion.

Identify an incident response team (e.g., CIO, Data Coordinator, IT Manager, legal counsel).

Outline steps needed to identify and contain the breach, catalog the lost data, identify what leakage has occurred and how.

Should you notify potential victims? When / how? What legal requirements exist? (Plan to assure compliance with any such requirements.)

What corrective actions should you implement to prevent a breach recurrence?