Update 1:

Nothing to see here …

The district’s file transfer server appears to be normal. Nothing is out of the ordinary.

The site uses FTP and requires a valid username and password to access the service. Only certain limited users at the district and community college have access.

Note: File Transfer Protocol (FTP) does not encrypt or protect any data sent using the service.

The professor at the college confirms that Daniella did not fail her course,

The calculus professor states that the grade she has marked down is correct and does not know how the grade at the district became different from her gradebook.

John, who is the person at the community college who sends the transcripts back to the district, confirms that he sent the grades properly and on time.

Update 2:

Bullies …

One of the bullies admits the entire thing was an attempt to get back at Daniella for being a better student than the two bullies.

The other bully performed a Man in the Middle (MitM) attack and was able to obtain John’s password.

They then used the coffee shop to log into the district server and replace Daniella’s grade.

Develop Incident Response Plan

Use your notes from the scenario discussion.

Identify an incident response team (for example, 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 and how? What legal requirements exist? (Plan to ensure compliance with any such requirements.)

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