Update 1:

Extra… Extra… Read all about it!

The local newspaper runs a story with the headline*: “Privacy Nightmare:* *Students’ Data Leaked on Website.”*

The story contains pictures of the school’s application website displaying a form clearly containing FAFSA data. The student’s data have been redacted, but the picture clearly displays a filled form containing data.

When contacted about the story, the reporter a student tipped her off, and then she accessed the data herself. She claims that she did not save or store any of the data she accessed.

Update 2:

When Good Updates Go Bad

The application manufacturer recently provided a product update that applied an enhanced search feature and fixed some bugs with storage and permissions.

A byproduct of the update was that it reset default permissions for certain files and folders, and the default permissions were “world readable.”

In this case, these files could not be altered or written to but could be accessed and read by anyone. This was mentioned in the patch notes but was buried in small print.

Press Release Time

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

Your spokesperson will read your press release to address the issue and then take questions.

Your audience includes reporters from local and national media, as well as students (victims), privacy advocates, and activists.

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?