Update 1:

The Infection Spreads…

Your information systems continue to be infected despite your best efforts to curtail internet access. Systems which are not logged into by enterprise users are turning up infected. It appears that this malware is spreading on its own.

One server is infected. You don’t know what’s on it, but it may have old copies of individual student-level data (personally identifiable information).

There is a patch for the vulnerability that would prevent further spread of the infection. It was released two months ago but some machines in the organization have not received it.

Update 2:

Production machines and servers are affected…

Several production machines, including a key database server, are now affected by the malware. Normal operations are hobbled.

It’s time to decide whether or not to pay…

Update 3:

Extra! Extra! Read all about it….

The local paper runs a story with the headline “Computer Systems Crippled by Recent Ransomware Attacks!”

The article describes the statewide longitudinal data system (SLDS) is affected and insinuates that the entire organization’s data are corrupted and are no longer accessible. Reporters are calling, and privacy groups are asking your public affairs contact whether your organization paid the ransom and demanding a response about any potential breach of student data.

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?