Southern New Hampshire University

CYB 200 Project Two Scenario One

You are a member of the information security team at a large financial organization. Last week, your team responded to an incident reported by a panicked payroll administrator. As she returned from a coffee break, the administrator witnessed a suspicious-looking person rush out of her office and leave the building via an emergency exit. The person wore a backpack (seemingly full) and clutched a small, "weird-looking" electronic device.

The payroll administrator immediately noticed that the office's file cabinet drawers were ajar, her workstation was turned sideways, and her USB headset was unplugged. The incident report listed some additional facts:

- Half a drawer of manila folders (contents unknown) were missing from the file cabinet.
- Remote access logs indicate that several foreign connections were made to the corporate network using the payroll administrator's account on the very same day she reported the incident.
- Payroll reports generated the day after the incident contained "inaccuracies" that are being investigated by the human resources office.
- The organization's payroll application is suffering from unexplained outages that last anywhere from a few minutes to several hours.