EOC Team Meeting June 21, 2016

Cyber Attack TTX

Scenario

- 7-8 AM, 2 days prior to graduation/ before term started
- Files encrypted
- Disconnect machines from network. (Don't shut down)

Incident vs. Breach

Incident-Something is happening

Breach= Data is moving out of the network to an external source

Incident was found but breach had not occurred.

Actions: CSIRT Computer Security Incident Response Team, Chief, Carlos, Neil, M. Berman, and Herb determine how severe the threat is.

(These are not in order of importance or execution)

- Caution on the side of Error for response.
  - The over elevated response insures relative legal safety
    - **Notify**, for legal reasons (be wary of systems acting up, downloads)
      1. Basic info. (What's happening)
      2. Stand-by for instructions
      3. Life Safety Issues
    - Engage OOG Council
    - Protect campus CSU
    - Insurance needs to have needs to have proof of notification.
- Activate the EOC
  - Which Positions
    - Finance (We might need computers, or additional equipment, personnel)
    - Equipment for response
  - Does it need to be activated "off campus"?

- ID Key Resources
  - Systems that's ARE vs. AREN'T affected (have the potential)

    ARE→ Certain computers, network files (G Drive), Door Locks (will go on battery), Files in CI Learn, WIFI

    AREN'T→CI Alert, The Web Page, Crucial Life-saving Systems (Fire Alarm,), Cash Net, STAR Rez, Parking?, All apps on myci,
- Assessment and Triage Needed

    - "Tear systems apart"
    - Attempt Remote Access

- Lock Down the Systems
    - Cash Registers (limited access/)
    - Police Info.
    - Others

Change to Scenario

(Attack/Incident Occurs on Saturday)

Issues:

1. How would anyone know it's actually happening if they aren't using their computer?
2. How do you determine if computer is under attack?

Actions:

- If computer is suspected of being infected (acting oddly/ file issues), DO NOT TURN OFF Computer.
    - Erases forensic evidence.
- Computers that are off during the duration of attack (Class room computers that weren't in use) are most likely safe

Questions

Do we pay the ransom?

NO.

-We have back-ups…hopefully.

-We can back-up from 24-hours before the incident.

Do we still have classes?

Yes, have classes. It would be more disruptive to not have them.

Prices?

Could be very expensive.