RANSOMWARE PLAYBOOK

You just received a rather panicked call from a respected PI detailing that her computers used for climate modeling sponsored by NASA have been hit by ransomware. This ransomware seems to have infected and then encrypted all her data, including her external hard drive backups. According to the ransom she received, she must pay the $10,000 ransom in a week or the encryption key will be deleted and the data lost forever.

Identification:

- Immediate action to limit damage to other systems; physically remove all affected and suspected affected machines off of the network. What other shares, systems did/do they have access to.
- Preliminary data assessment: In this case it is not PII, but could be highly sensitive for proprietary, research or contractual reasons. Scope in this case is limited to this lab/researcher.
- Quick documentation of the situation logged. Ticket produced with all timings and action taken thus far logged. From here on all activities should be logged in incident ticket and ownership deliberately transferred.

Containment:

- Incident responders and management notified. Incident responsibility likely passed to senior staff. Team would include at least one member of Lvl1(service desk, comms), Lvl2 (boots on the ground), security (coordination, enterprise system log collection).
- Verify scope and assurance on containment. Probe infection vector (email, browsing, usb key, etc.) to help with containment.
  - Email: Immediately report to phishing.reponse, security.response@utoronto.ca, and Teams, possibility for wide spread damage.
  - Browsing:
  - USB Key: Strongly consider community notification, certainly department or UTM Status notice on short notice.
- Detailed assessment of information: What is the scale, scope? In this case, likely, a very large volume of important research data.
  - Report to ISEA – security.response@utoronto.ca
  - Report to Departmental Chair
  - Reporting to I&ITS Departmental Management
  - Follow contractual reporting requirements for reporting to NASA, other stake holders. (At least begin the process of doing so while other steps are taken)
- Log and evidence collection
  - Gateway firewall logs keep copy for later investigations as well as use to ascertain if there was any data exfiltration.
  - Gather as much evidence as possible. Campus police door access logs? Other system logs, AD Audit full ‘relevant’ authentication history, Wireless logs for all relevant devices, accounts. Associated network traffic logs. Running processes, netsh sessions, etc. (Incident captain will store all evidence)

    - Can we get a copy of the malicious file(s)? Knowing flavor of crypto locker is key to recovery.

Eradication and Recovery:

- Further verify that other connected systems are not affected.
- Depending on method of infection, similar systems need to be checked out and verified clean and secured. (Was it a patching miss, a physical attack, phishing oriented, did it involve rights escalation that should not have been present, etc)
- Restore system – ideally with known good backups. May involve a clean rebuild of everything.
- Investigate and utilize public tools/methods available for this flavor of ransomware.

Communications:

- Communications in this case will revolve around key lab stake holders, departmental and UTM leadership, ISEA, and any contractually required parties based on the particular data.
- Depending on nature of the attack particulars (eg.evidence of exfiltration, highly sophisticated attack), method of entry, scale of exposure, law enforcement may need to be notified.

Follow up:

- Complete documentation for incident, including chronology of events.
    - Again, depending on particulars, team would work with stake holders to put additional controls and implement lessons learned.
    - Questions may include: Why was the data not backed up? Why was the system configured or used as it was? Why was the compromise allowed to occur?
    - Who is responsible for each of the remediation steps?
- Initiate remediation plans, assign deliverables.
- Securely store all incident documentation, logs, and other evidence.