CIRT Playbook Battle Card: **GSPBC-1010 - Device Theft - Device Loss**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain an up to date inventory of electronic devices
4. Place asset tags on company owned devices
5. Make use of full disk encryption
6. Set password/pin policies on devices
7. Maintain the ability to remotely wipe devices
8. Be aware of any laws or contractual obligations requiring notification of data loss

(I) Identification

1. Monitor for:
    a. Employee reports of device theft/loss

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Determine:
    a. What data was stored on the device
    b. How data stored on the device is protected
    c. What remote data and services are accessible from the device
5. Change the passwords of any accounts used on the device
6. Review logs for unauthorized activity from the stolen/lost device or accounts associated with it
7. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Perform a remote wipe of the device

(R) Recovery

1. Restore to the RPO within the RTO
2. Notify third parties of data loss if appropriate
3. Notify law enforcement if appropriate
4. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx

GUARDSIGHT