12/3

Incident Response

Plan:
- Business Continuity Plans - keep going
- Disaster Recovery Plans -

Preparation
- Redundant Sites
  - Hot site: duplicate of live system
  - Warm site: update data, start system
  - Cold site: equipment set up data restoration

(2)

Incidents:

precursors:
- port scans - check for services
- new exploit/vulnerability

indicators:
- data that attack is occ.

isolation/containment
- disconnect device
- lock account (don't delete)

Recovery
- remove malware
- erase/replace

Remediation
- make sure it doesn't happen again
- find other precursors/ indicators

Report & Disclosure
- documentation