“Components of an Incident Report

@UMCST

Include the following information:

- Timeline of events
    - date/time the attack started (if known)
    - date/time the attack was discovered
- attacker source address(es)
- target system(s) name and targeted address(es)
- target port / service
- type of attack
- result of attack
- Vulnerability / configuration that allowed the attack
- how discovered
- how contained
- remediation
    - Planned and/or implemented actions / controls
    - result of remediation