Bare Bones:
Incident Response Plan

STEP
01

Structure of Incident Response Team

- Know members and their roles
- Designate 'responsible parties' who will own the IR processes
- List parties that might need to be alerted
- Identify under what circumstances they will be alerted

STEP
02

Define what Constitutes an Incident

What threshholds have to be passed to move something from an event to an incident. Every organization with a developed plan defines this differently, Figure out what works for your organization

STEP
03

Identify steps taken during all stages of Incident Response

- First, events are recorded in a ticketing system
- Then, all events are evaluated by some member of the team
- If the threshold is passed, the IR team is activated and these business officers are alerted

STEP
04

Establish a Documentation Methodology and Repository for all Incidents

This includes after action reports and root cause analyses that occur after closing an incident.

STEP
05

Create a Schedule

- Put it to the test
- Update plan

SECURE HALO
SECURING THE ENTERPRISE

#CyberAware