JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Finishing the Response

CYBER INCIDENT RESPONSE

Finishing the Response

- Change Management Process
- Lessons-Learned
- Final Report

Change Management Process

- Emergency Change Management Board may have authorized numerous actions during the incident response
- Follow-up to ensure all changes have been documented properly
- Need to ensure that network diagrams and vulnerability scan profiles updated

Lessons-Learned

- Documents the details, the root cause, and the solution to a security incident
- Fact-finding meetings should be conducted as close to the end of an incident response as possible
- Needed changes identified during the lessons-learned process should be fed into the resourcing and Change Management process

Final Report

- Every incident should finish with a compiled written report
- Established organizational “memory”
- Can serve as documentation in case further legal action occurs in the future
- Can identify other deficiencies in the incident response that need to be addressed by management

Final Report Includes...

- Timeline of incident and response events
- Root cause of incident
- Location and description of evidence
- Actions taken to contain, eradicate, and recovery (and the reasoning for them)
- Estimated impact to organization ($,time)
- Post-recovery validation effort results
- Documentation of lessons-learned

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE