Level 2 Block 5 Exercise Details
Large Group
Simulated Technology Failure Scenario

1. Mission Objective:
Each group to develop (1) IT incident response scenario to be exchanged with another group during breakout session. Unified Command will be simulated in the main session by Blackrock 3 staff.

2. Breakout Room details: Assigned Roles: IC, LNO, Scribe, LKT.
IC: Drive discussion and delegate tasks.
LNO: Provide briefings as directed in #3 and #4.
Scribe: Capture details and key events of the discussion and deliverables listed in #4 and share details of notes/timeline at the end of the briefing.
LKT monitors incoming broadcast notices from the main room.

3. Exercise Parameters:
- GL drives group discussion to draft a written description of a past, present or potential IT incident response scenario.
- Scenario must be written electronically on word processing application such as Google Doc/MS Word. Scenario must include enough specific and accurate detail to convey the signs and symptoms of the current conditions. **Assigned LNO should capture the scenario on their local desktop.**
- The group does not provide resolution actions or needs in this document.
- Once scenarios are drafted by each group, LNOs of each group are exchanged by returning to the main session.
- Lead instructor will move the LNO's to the appropriate groups for briefing.
- Each LNO briefs the new group on the problem statement and answers any qualifying questions about the scenario.
- Once briefing task is complete, LNO returns to the main room and is returned back to the original group by the lead instructor.
- Once each group has received the scenario and briefing, IC drives forward a discussion about resolving the scenario. There must be a primary resolution plan and a contingency resolution plan (Plan B). **See example below as a template for drafting the problem statement.*

Customer Service Representatives (CSR's) are unable to log into the billing application to processor customer payments. This issue is only impacting new users trying to sign in; users already logged into the application are not impacted. The issue is impacting approximately 300 CSR's in the Northeast Division for our biggest customer. The incident was discovered at 09:00 CST. Initially, this was thought to be an issue on the client side as some IP changes occurred around the same time the issue started. However, after the change was reverted the issue persisted. All other desktop applications are functioning normally; Currently, the only impact is to the billing application.

4. Minimum Exercise Deliverables:

- Identify SEV or P level for the incident.
- Create a list of SMEs, vendors, Executives, etc. that would be dispatched to the incident.
- Draw an org chart depicting all the incident responders identified above.
- Draft an overall Mission Objective for the response.
- Draft a CAN report for the primary resolution plan and Plan B.
- Identify any unique aspects or challenges of the response that may pose a challenge to the resolution effort.
- List the cadence and potential audiences for any LNO briefings that need to occur outside the resolution effort.
- LNO delivers the scenario briefing back to the entire group in the main session at the conclusion of the exercise.
- LNO drafts (1) LNO briefing representative of the beginning, middle or end stage of the incident (same type of exercise as seen in Block 5, Level 1 Incident Commander Training).