Team Leadership

Jeremy Sparks
Intro

- Disclaimer

- Work Experiences
  - AFCERT
    - APT intrusions
    - Insiders
    - DDoS
    - Outages (Network & Weather)
  - IT upgrades
Problem Statement

- Scale of network & threats plus:
  - Lack of focused IT leadership training
  - **Critical** self-analysis missing in our community

- Solution and results
- Scope of the solution
The Basic Principle

**PLAN**
- Endstate: Outline of the effort / mission

**BRIEF**
- Endstate: All team members understand the plan

**EXECUTE**
- Endstate: All expected tasks completed

**DEBRIEF**
- Endstate: Lesson Learned / Best Practices identified
“If you fail to plan, you are planning to fail.”

Benjamin Franklin
Planning

- Good leaders are good planners
- Problem: Most people feel very uncomfortable as planners
- We discovered that it is best to have a structured planning format
  - Keeps it standardized
  - Becomes muscle memory
- SUCCESS = Everyone on your team is comfortable with planning
- Our method
Lead the planning effort/team

- Mission
- Enemy
- Environment
- Effects
- Capabilities
- Plans / Phases
- Contingencies
- Communications

If the plan sucks, you can only blame yourself
Example Plan

Spoiler Alert
**ROC DRILL Timeline**
- Access granted
- APT detected
- Compromised account located
- Password reset initiated
- Access lost
- Services drop
- Main Server Crash
- Tools don’t work
- Pen test success/failure
- Customer PII leaked
- Customer complaints pour in

**Specific / Anticipated Communications**

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Authority</th>
<th>Communications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Comp PWD</td>
<td>IT Dept</td>
<td>“PWD X locked out”</td>
<td>IOC added</td>
</tr>
<tr>
<td>2.</td>
<td>Access needed</td>
<td>IR Lead</td>
<td>“Access - System X”</td>
<td>IT Dept confirms</td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Comm Plan**
- Pri/Sec/Ter Comms
- Trigger points & procedures to transition to backup Comms
- Brevity
- Call Signs
- Collaboration (VTC, Corporate IM, SharePoint)
- Deliverables produced during/after Execution
- Format
- Suspense
Lead by briefing the team

- Mission Leader Conveys Plan
  - Cover the whole mission
  - Opportunity for team to ask questions/weigh-in on planning

- Brief includes:
  - Team objectives, tasks & expectations
  - Assessment plan
  - Visual timeline of events
  - Roles/Responsibilities/Resources
  - Assumptions and Contingencies

The brief sets the tone for the whole effort
Lead during execution

- Execute in accordance with established guidelines & procedures
  - Directive Guidance
  - Checklists
  - Company policies
- Everyone should be noting observations throughout
  - Driven by assessment planning
  - Leader can assign focus areas to individuals

Deviations OK, but should be debriefed
“Those who cannot remember their mistakes are condemned to repeat them.”

George Santayana
Lead the Debrief

- Reconstructing / analyzing an event to avoid repeat mistakes & clone success
- Led by leader; entire team participates & Rank is a non-factor!
- Tied to overall plan/objectives
  - Did we stick to the plan?
  - Was the plan sufficient?
- Structured Flow
  - Repeatable
  - Aids in avoiding pitfalls/bad habits
Debrief Basics

- A.K.A. a Hotwash or AAR
- Busbahnhof vs. Postbahnhof
- Institutional learning
- Must be internally focused
- Salad Gate 2011
- The Bathtub faucet
Common Debrief Mistakes

- Not internally focused
- Jumping to Fix Action before identifying the Root Cause
  - Avoid: “I already know what went wrong…Here’s simply what we do”
  - You can have suspicions, but always run through the process
- Not owning up to mistakes
  - Leave your ego and self preservation at the door!
Dinner Party Example

- **Objectives**
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine

- **Specified Tasks**
  - Make dinner
  - Provide entertainment
  - Clean the house

- **Implied Tasks**
  - Decide what recipes to use
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games

- **Constraints & Restraints**
  - Has to end before baby's bath time
  - Can't serve alcohol to minors

- **Assumptions**
  - All guests will be omnivores
  - Guests do not have food allergies

- **Assessment Criteria**
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it's babies bath time and have to leave
Dinner Party Debrief

Reconstruction

- 0800 – woke up
- 1200 – ate lunch
- 1300 – wife and I begin cleaning
- 1345 – note: cleaning taking too long
- 1400 – baby is fussy
- 1400 – I start taking care of baby
- 1445 – baby falls asleep (finally)
- 1500 – left for the grocery store
- 1600 – return from store/start cooking
- 1645 – noticed missing key ingredients
- 1650 – used soy sauce for beef bouillon
- 1715 – Set table/prepare entertainment
- 1730 – guests begin arriving
- 1830 – Dinner served
- 1845 – guests hardly touched food
- 1850 – subject of food quickly deflected
- 1930 – guests only mingling/party dead
- 1945 – guests leave earlier than plan’d

DFP: Why did the guests dislike the food? (Obj 1 & 2)

- The guests’ tastes are subjective
- I failed to feed them delicious food
  - I failed to prepare the food in accordance with the recipe
    - I did not have all of the ingredients
    - I failed to purchase all needed ingredients needed when at the grocery store
    - I didn’t know better

IF: create grocery list with required ingredients

Lesson Learned: When preparing for a dinner party, I will remember to buy all of the required ingredients by creating a grocery list to remind me of what ingredients are needed so that the guests will like the food.
Dinner Party version 2.0

- **Objectives**
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn’t interfere with baby’s routine

- **Specified Tasks**
  - Make dinner
  - Provide entertainment
  - Clean the house

- **Implied Tasks**
  - Decide what recipes to use
  - Make a grocery list
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games

- **Constraints & Restraints**
  - Has to end before baby’s bath time
  - Can’t serve alcohol to minors

- **Assumptions**
  - All guests will be omnivores
  - Guests do not have food allergies

- **Assessment Criteria**
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it’s babies bath time and have to leave
Dinner Party 2.0 Debrief

Reconstruction
- 0800 – woke up
- 0900 – made ingredient/grocery list
- 1200 – ate lunch
- 1300 – wife and I begin cleaning
- 1500 – left for the grocery store
- 1600 – return from store/start cooking
- 1715 – Set table/prepare entertainment
- 1730 – guests begin arriving
- 1830 – dinner served
- 1845 – conversation is lively/jovial
- 1900 – most guests plates empty
  - 1900 – guests A, C, & D asks for seconds
  - 1900 – guest B has only eaten salad
  - 1900 – guest B looks frustrated
- 1915 – All guests enjoying party games
- 1930 – guest B snacking heavily - veggies
- 2045 – guests have to be kicked out
- 2100 – baby put to bed

DFP: Why guest B dislike the food? (Obj 1 & 2)
- I failed to prepare food to her liking
  - I failed to assess guest food preferences or diet restrictions
    - I didn’t know better
  - I failed to give the guests food options
    - I assumed all guests were omnivores
      - I didn’t know better

IF: make a contingency plan for guests that may want/need other food options

LL: When planning for a dinner party, I will not only plan for everyone to like the same type of food by having a contingency plan in place for people who may want/need other food options (e.g. vegetarian) so that every guest enjoys the dinner.
Dinner Party version 3.0

- **Objectives**
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine

- **Specified Tasks**
  - Make dinner
  - Provide entertainment
  - Clean the house

- **Implied Tasks**
  - Decide what recipes to use
    - Include vegetarian recipe
  - Make a grocery list
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games

- **Constraints & Restraints**
  - Has to end before baby's bath time
  - Can't serve alcohol to minors

- **Assumptions & Contingencies**
  - All guests will be omnivores
    - Have vegetarian option

- **Assessment Criteria**
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it's babies bath time and have to leave
Challenges

- Corporate anti-bodies to change
- Lack of qualified planners
- Egotism in the debrief
Takeaways

- PBED may seem daunting at first, but you will get better over time
- Don’t fight the process, trust in it
- If you repeat a problem even with implementing an FA, then:
  - You did not find the true root cause or FA was not sufficient
- Archive your previous executions & previous LLs
- It’s an operational rhythm… more importantly, it’s a lifestyle / culture
- The magic is in the debrief
Questions?