RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HUM-F01

# Train Like You're Going to Fight

# What Kind of Exercise Meets Your Needs?

**Dr. Joe Adams**
Vice President for Research and Cyber Security
Merit Network, Inc.

#RSAC

# Agenda



- What is this talk about?
- Exercises in Context
- Type of Exercises
- Putting Cyber in Kinetic Exercises
- Getting Your Exercise Started

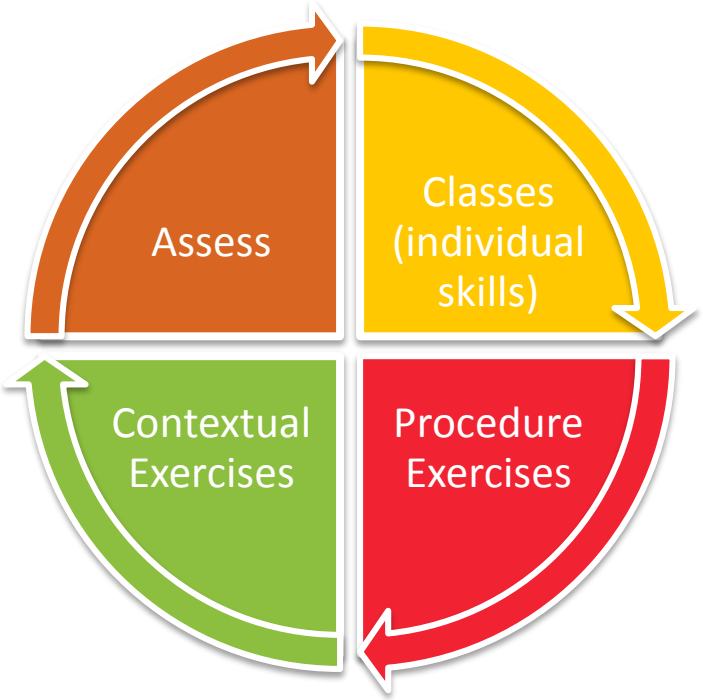
# Introduction



- **Why you're here**
  - Talk about which type of exercise suits your objectives
- **What you'll take away from this presentation**
  - Steps to create an exercise
  - Survey of exercise types
- **Why this is important**
  - Validating processes in a controlled environment

merit

# Training Cycle



# Why you need to exercise

- Complements classes
  -- Crawl -> Walk -> Run
- Validates & reviews processes
- Practices procedures – team dynamics
- Delivers a big picture view of a process or situation

# What you need to exercise



- Legal/Policy
- Media Engagement/Breach Notification
- Insurance coverage
- Response plans

- Not purely technical!
- Get everyone involved!

merit

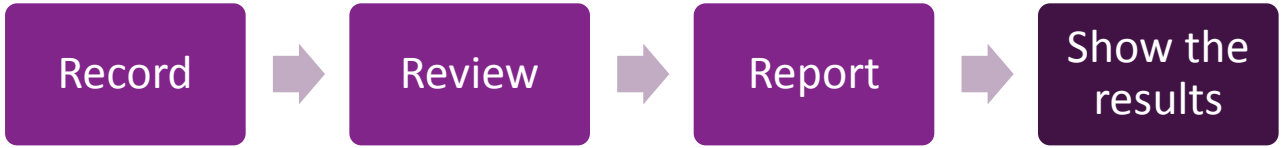
# Who needs to participate?

- Managers across the company
  - Sales & Marketing
  - Finance
  - IT
- IT staff
- DFIR teams

merit

# The Key Components






***Make it worth the time!***

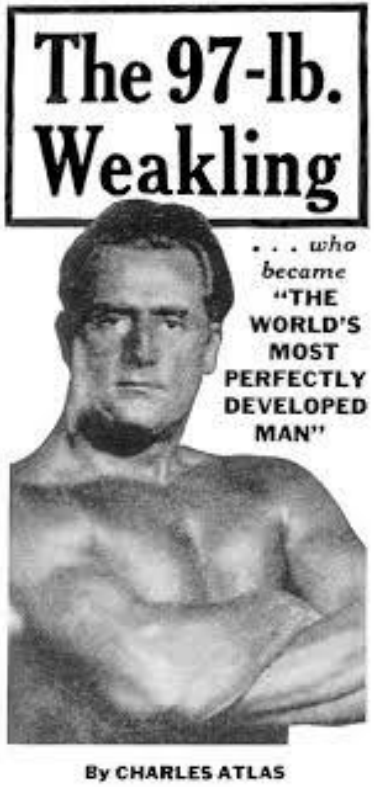
merit

# What gets in the way

- Budget
- Time
- Experience in putting an exercise together
- Unwarranted belief in untrusted skills

# Who else does exercises?

- The usual suspects: Government, DoD, DHS
  - Usually kinetic. Increasingly including cyber
- Healthcare, Finance
  - Moving from tabletop exercises to more hands-on CTFs
  - Demonstrate planning and response
- Utility Companies
  - Large & medium sized companies (CIP v5)

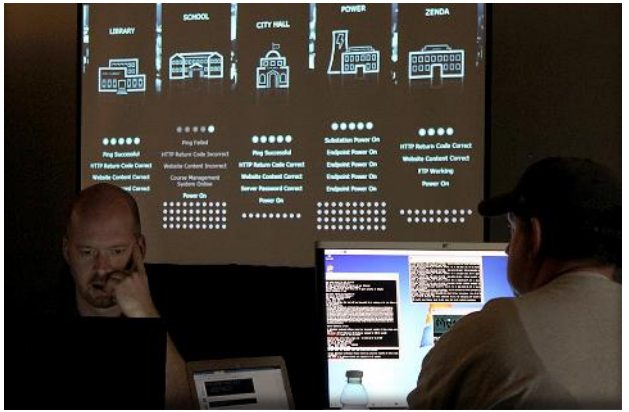



merit

# Types of Exercises

# Types of exercises

- Table Top Exercise (TTX)
- Capture the Flag (CTF)
- Red vs Blue
- Red on Red
- Incident Response (DFIR)



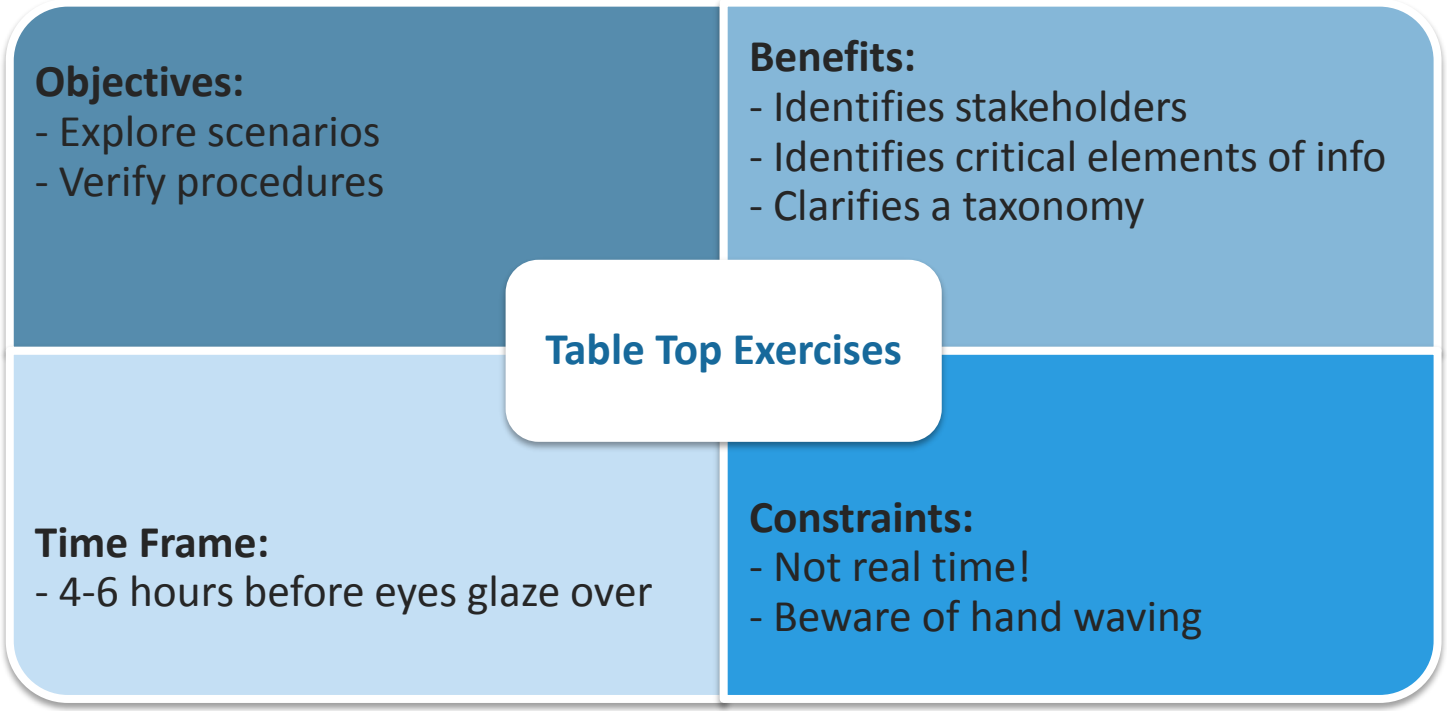
# Table Top Exercises



- Just like it sounds
  - All you need is a table
  - Use a note taker
- Applicable to:
  - All levels (technical through executive)
  - All sections (make the geeks talk to accountants!)

# Table Top Exercises





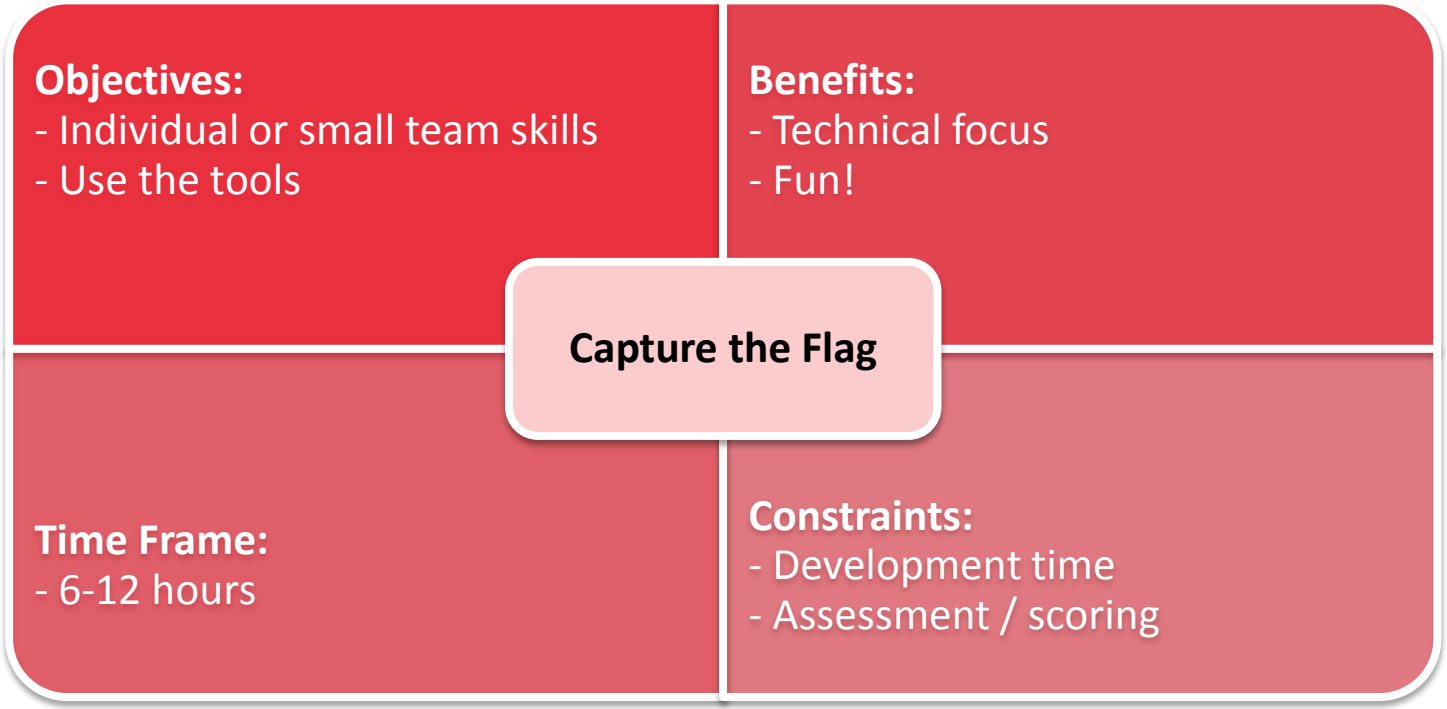
# Capture the Flag

- Technical
  - Seen at most (all?) hacker conferences
  - Does everyone get a copy or is it a shared environment?
- Applicable to:
  - Recruits
  - Students
  - Technical staff

merit

# Capture the Flag

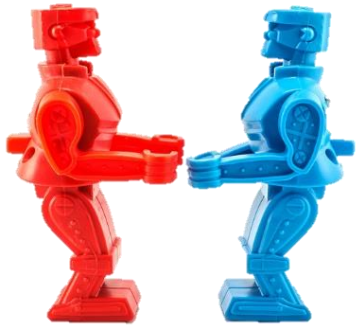




# Red vs. Blue

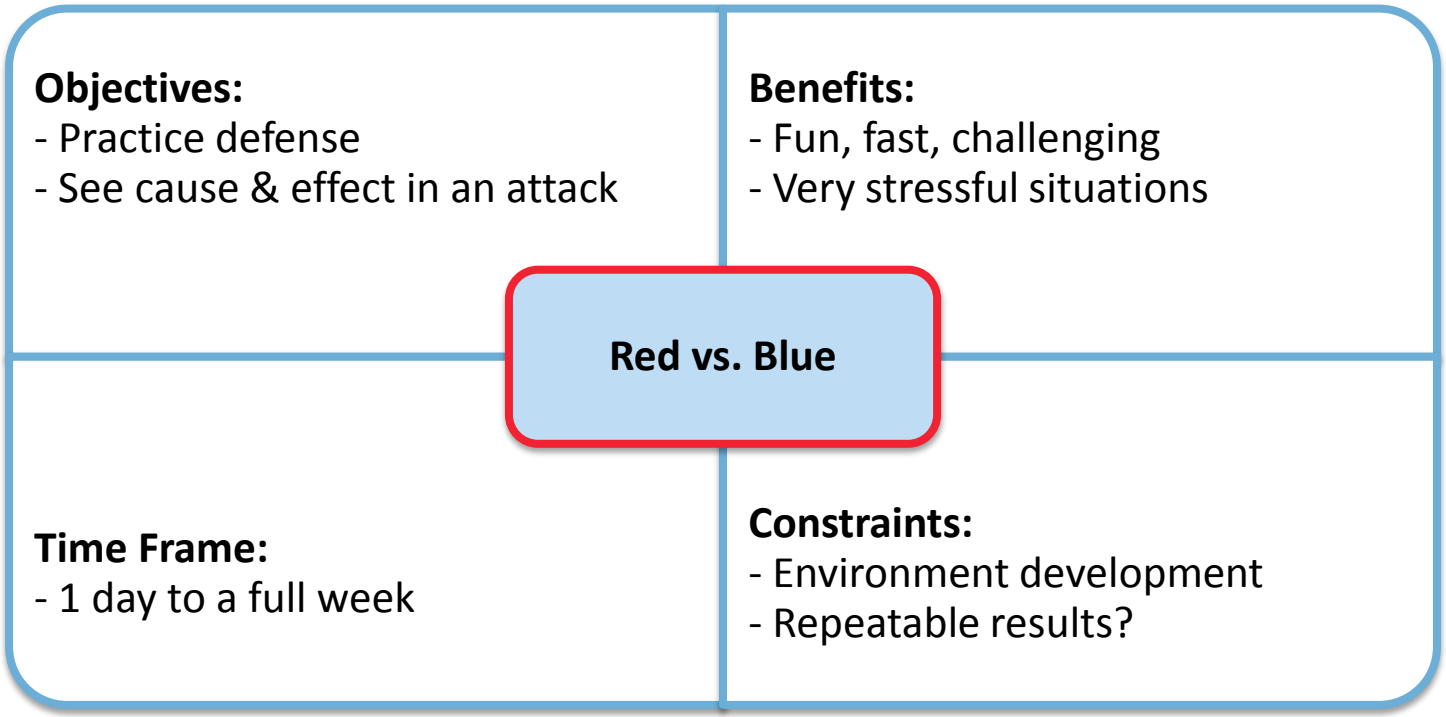


- I attack, you defend
- Run locally, run nationally
  - Cyber Patriot
  - National Collegiate Cyber Defense Competition
  - Inter-service Academy Cyber Defense Exercise
- Applicable to:
  - Students (culmination event)
  - IT Teams



merit

# Red vs. Blue

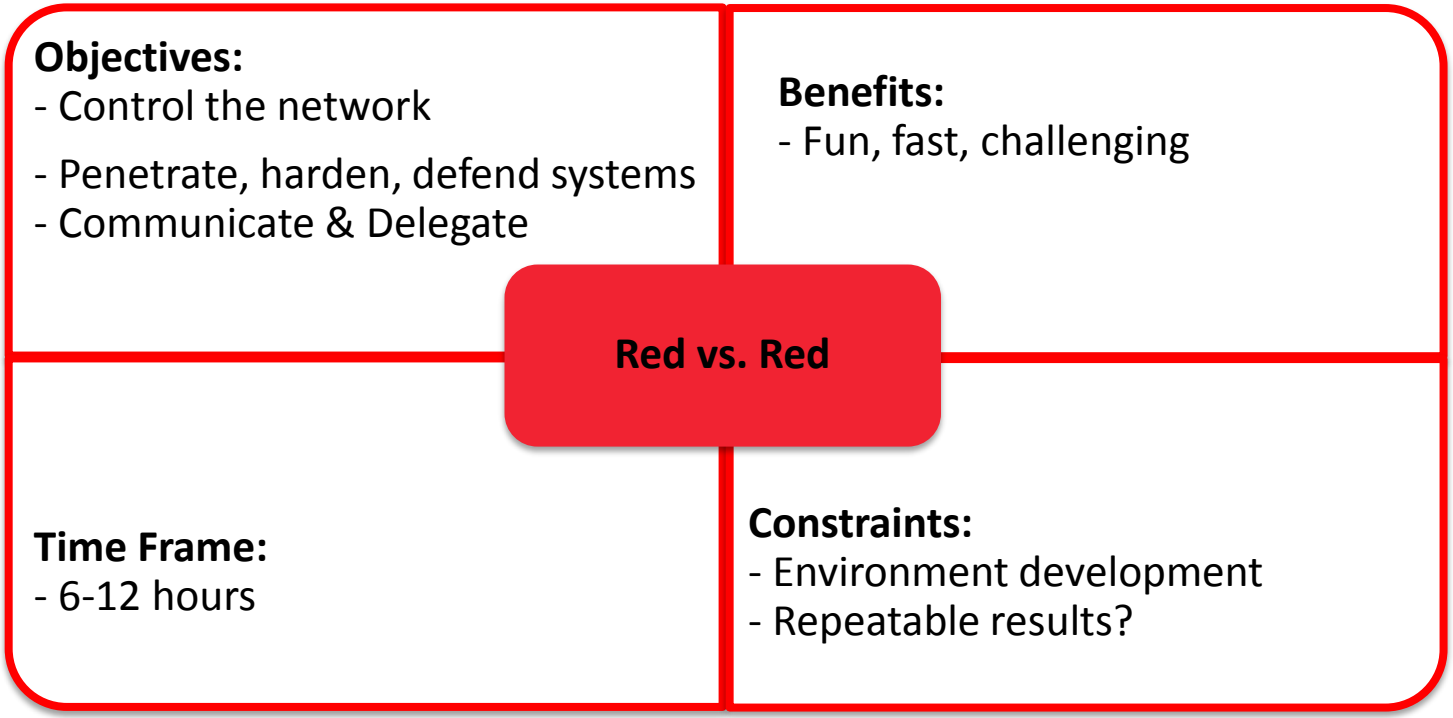

Objectives:
- Practice defense
- See cause & effect in an attack
Benefits:
- Fun, fast, challenging
- Very stressful situations
Red vs. Blue
Time Frame:
- 1 day to a full week
Constraints:
- Environment development
- Repeatable results?

# Red vs. Red



- Paintball – everyone attacks and defends
- Can get very chaotic!
- Applicable for:
  - Advanced students
  - Pen testing teams

# Red vs. Red


Objectives:
- Control the network
- Penetrate, harden, defend systems
- Communicate & Delegate
Benefits:
- Fun, fast, challenging
Red vs. Red
Time Frame:
- 6-12 hours
Constraints:
- Environment development
- Repeatable results?

# Incident Response



- Something bad happened
- Needs a lot of prep or a lot of time
  - Do you give them disk images?
  - Can you generate enough, realistic, log data?
- Applicable for:
  - Incident response teams
  - Generating results to inject into a TTX

# Incident Response



**Objectives:**
- Validate Incident Response plans
- Perform DFIR skills
- Rapid familiarization of a network

**Benefits:**
- Practice DFIR
- Demonstrate what IR teams do

**Incident Response**

**Time Frame:**
- Days, especially if evidence collection is included

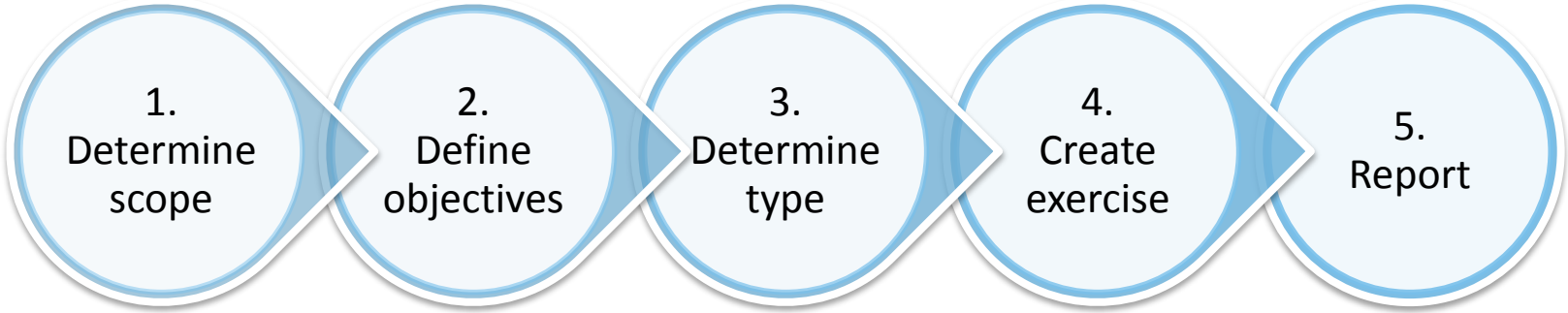
**Constraints:**
- Environment development

merit

# Steps to Making an Exercise - Overview

# Don’t Panic!

# Making an Exercise



# Making an Exercise



- **Sponsor**
  - Who are we going to report the results to?
- **Scope Definition**
  - What are we going to exercise?
  - Who needs to be involved?

# Making an Exercise



- Objective Definition
  - Here's what we want to test
  - Here's how we'll test it
  - Here's what we think you're going to do
  - Here's what you did
- Task – Condition - Standard

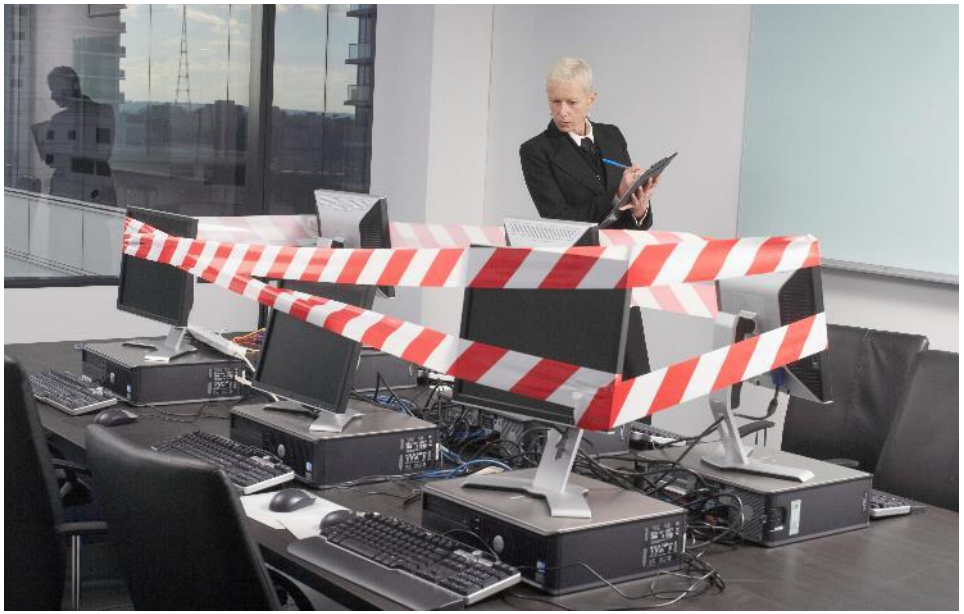
# Making an Exercise

- Decide which type of exercise suits your requirements
  - Table Top Exercise
  - Capture the Flag
  - Red vs Blue
  - Red on Red
  - Incident Response

merit

# Making an Exercise

- Create the Scenario
  - Realistic
  - Applicable
  - Keep it Simple!



# Making an Exercise



- Other Documentation
  - Master Scenario Events List
    - Timeline
    - Communications
    - Governs the flow of information
  - Evaluation Guide

# Making an Exercise

- Write the Exercise Directive
  - Objective Definition
  - Scenario
  - Means of Communication
  - Timeframe
  - Evaluation/Assessment

# Making an Exercise



- Publish the Exercise Directive
- Location
- People
  - Participants
  - Facilitator/Evaluator

# Making an Exercise - After



- **Hotwash**
  - Immediately after the exercise
  - Get everyone's impressions, perceptions, gripes, and kudos
  - Answer the sponsor's question: "So how did it go?"
- **After Action Review**
  - Walk through each objective and inject
  - Results in a report with
    - Record of what happened
    - Follow ups and due outs

# Cyber in Kinetic Exercises



- Start small: don't derail it or you won't be invited back
- Stay with published exploits: if you claim "0 Day", you'll get called out
- Target specific systems/effects = task-condition-standard
- Manage expectations to make sure they know what's coming

# An Example of an Exercise

# An Example



- Sponsor – Company CEO
- Scope - Small company, all sections/directors (about 14 people)
- Objectives - Continuity of Operations
  - Do you have plans in place if the company is displaced?
  - Where is the company's data?
- Type – Table top exercise

# An Example



- Created a simple scenario
  - Three phases
- Created injects in the form of questions
  - Assigned responsibility for each inject
- Scheduled 4 hours in a conference room
  - Included a scribe with a laptop
  - I facilitated – focus on communication between teams

merit

# An Example

- Scenario – A fire in the office
  - Phase 1 – The fire is happening
    - Reporting
    - Information dissemination
  - Phase 2 – The inspection
    - Temporary location (1 week to 3 months)
    - What information is needed?
    - Information access
  - Phase 3 – The clean up
    - Prolonged displacement (3 to 6 months)

# An Example



- How it went
  - IT was defensive
  - Finance and Sales were curious (over confident?)
  - Marketing was the least prepared
  - 5 hours
- What we discovered
  - No backups in Marketing
  - Many leave their laptops in the office (information access)
  - IT relies on email to communicate and doesn't have a backup plan

merit

# An Example



- The follow up
  - Cloud-based backups
  - Emergency procurement processes
  - Alternative communications paths
- Still working on
  - Alternate locations
  - Data access issues for specialized applications

merit

# Apply what we've talked about



- Next week
  - Pick 3 processes that need to be exercised
  - Assess your organization
- Within 3 months
  - Develop a Table Top Exercise
  - Deliver the results to potential sponsors
- Within 6 months
  - Explore other, more in-depth exercises
  - Start to plan a training cycle

merit

# Summary

- Five types of exercises
  - Each exercise is different
  - Pick the type that addresses your objectives

# Conclusion



- Let objectives drive what type of exercise
- Get everyone involved
- Resources and time will scale the exercise
- Reports and follow up are key to holding the next one!

merit

# Questions?

# Contacts


- Dr. Joe Adams
- cyberrange@merit.edu
- www.merit.edu/cyberrange

merit.edu
Teach. Test. Train.

merit