# Designing Cyber Exercises

Longo / Gregory

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

Approved for public release, distribution unlimited.

The original document contains color images.
CWD Mission

Provide force-multiplying solutions...
To rapidly grow the nation’s cyber workforce...
Addressing the problems of time, scale, and cost
CWD Perspective

CWD Challenges

• Vulnerabilities, threats, and technologies change so rapidly
• Unlike adversaries, rule of law limits full freedom of maneuver
• Traditional “Brick and Mortar” training models
  – Difficult to train regularly due to logistics/budget restrictions
  – Doesn’t scale across a globally distributed workforce
  – Difficult to “train as you work” routine
  – Difficult to assess individual/team readiness routinely

CWD Research/Solutions Focus

• Focuses on the problems of time, scale, and cost.
• Develop innovative methods to compress the time it takes to build cyber expertise and to amplify that expertise across a globally distributed workforce
• Emphasize individual/team readiness and effectiveness
Overview

• Background
• Why develop an exercise
• Types of exercises
• Planning
• Design
• Development
• Execution
• Supporting documentation
• Lessons Learned
Background

- **Knowledge, skills, and experience**
  - **Knowledge** building provides a solid foundation of knowledge; fundamentals and concepts
  - **Skill** building focuses on learning how to apply hands-on, technical skills
  - **Experience** building develops the ability to adapt and successfully apply skills in changing and unfamiliar environments; apply knowledge and skills in real world scenarios

- **Skill proficiency**

- **Training scalability**
  - Audience
  - Budget

Source: The CERT® Approach to Cybersecurity Workforce Development
Workforce Development Cycle

Figure 1: The CERT Approach to Cybersecurity Workforce Development
Why Exercises?

• Experience building
  – Safe environment
  – Repeatable

• Demonstrate capabilities
  – Integration of people, processes, and technology

• Experimentation
  – Tactics, techniques, and procedures

• Focus on process improvement
  – Organizational education
Proven Approach

• Exercises have been used to prepare for natural disasters and physical hazards for many years
  – Military “wargaming” → early 1800’s

• Homeland Security Exercise and Evaluation Program (2002)
  – Based on DOD training and exercise programs
  – Fundamental principles that frame a common approach to exercises
  – Unique challenges for cyber

• National Strategy to Secure Cyberspace (2003)
  – Cyber exercises identified as a critical component to develop public-private partnerships and evaluate cyber security continuity plans
Cyber Exercise Hurdles

• Requires operational realism to enhance value
• Lack of codified best practices leads to ad hoc formats and planning methodologies
• Unique complexities based on the technical nature of cyber exercises
• Rapidly evolving policies, actions, and doctrine
Definitions

- **Exercise** – a military maneuver or simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation*

- **Exercise Objective** – a specific statement of purpose, guidance, and/or direction for an exercise*

- **Cyber** – people, process, technology, and operations associated with digital information systems, networks, and data**

- **Cyber Exercise** – an exercise whose objectives primarily focus on protecting, defending, and recovering cyber assets and operations from a cyber attack or incident**

* Source: CJCSM 3500.03D, 15 AUG 2012
** Source: Methods for Enhanced Cyber Exercises
Exercises

• Influenced by organizational resources and exercise objectives

• **Discussion-based** focus on familiarization of plans, policies, agreements, and procedures
  – Tabletop Exercise (TTX)
  – Seminar
  – Workshop
  – Game

• **Operations-based** validate plans, policies, agreements, and procedures while clarifying roles and responsibilities
  – Drill
  – Functional Exercise
  – Full Scale Exercise
Exercise Complexity

**Figure 3: HSEEP Building-Block Approach**

Source: Methods for Enhanced Cyber Exercises
Foundation: Exercise Planning

- Executive and leadership support and commitment
  - Objectives
  - Resources
- Establish an exercise planning team
- Develop a project management timeline and clearly identify milestones
Building to the Event

Concepts & Objectives Meeting
- Exercise Description
- Exercise Objectives
- Stakeholders

Initial Planning Conference
- Participating Sectors
- Participating Organizations
- Organization Objectives (Sub-Objectives)
- Scenario Summary
- Threat Description
- Problem Sets
- Determine Ongoing Collaboration Needs

Mid-term Planning Conference
- Participating Organization Information (IT Assets, Security Posture, Participant Roles)
- Event Threads
- Event Details
- SimCell Requirements
- Train Ongoing Collaboration Tools (if necessary)
- MSEL Conferences

Final Planning Conference
- Review Final Documentation (SitMan, C/E Handbooks, MSELs, etc.)
- Perform Controller Training, Dry Run Events for Training
- Test Live Adversary Scripts

Source: Methods for Enhanced Cyber Exercises
Teams

• Planning teams are usually based on the type of exercise, complexity, scenario, location, and resources available

• Scalable 4-cell planning construct
  – Exercise Control (White Cell)
  – Threat Emulation (Red Cell)
  – Observer/Controllers/Evaluators (Black Cell)
  – Trusted Agents
Design: Objectives

• Well-defined objectives guide scenario development and evaluation criteria

• Exercise objectives (SMART):
  - Simple
  - Measurable
  - Achievable
  - Realistic
  - Task-oriented

• Most importantly, objectives should be specific and relevant
  “Identify potentially compromised systems that are communicating with an adversary C2 node via DNS.”

• Recommend limiting the number of objectives to ensure exercise is manageable
Design: Scenario

• The storyline that drives the exercise
  – Integration of realistic threats with a plausible story
  – Every aspect of the scenario should support specific exercise objectives

• Key scenario elements
  – Scenario objective(s)
  – Threat
  – Target
  – Operational effect (not necessarily business impact)

• Collaborative effort \(\rightarrow\) Trusted Agents (SMEs)
  – Threats
  – Cyber defense capabilities
  – Policies and procedures
  – Project and/or organizational considerations
Scenario Planning Methodology

- Phase 1: Develop Scenario Objectives
- Phase 2: Develop Scenario Storyline
- Phase 3: Develop Event Threads

Source: Methods for Enhanced Cyber Exercises
Key Scenario Elements

• Scenario objective(s)
  – Scenario objectives deconstruct exercise objectives into activities that can be developed as event threads

• Road to war – overview of the situation

• Threat
  – Actors and motivations
  – Live OPFOR
  – TTPs

• Target
  – Systems
  – Information/data
  – People
  – Processes

• Operational effect (not necessarily business impact)
  – Target effect
  – Discovery
  – Timeframe
Development: Scenario

• Master Scenario Event List (MSEL)
  – Chronological list of observable events during the exercise period

• Exercise event-level (lowest level)
  – Scenarios can have multiple event threads
  – Event threads typically have multiple events

• Event types
  – Threats
  – Injects
  – Player expected action
  – White-noise
Exercise Environment

• Exercise realism
  – Operational network v. cyber range
  – Scenario validation/plausibility
  – Systems and processes
  – Threat emulation
  – Traffic generation
Exercise Execution

• Exercise Control – maintain positive control of all activities including MSEL execution, ensuring objectives are met, and conducting briefings
  – Staffing from across the planning team
  – STARTEX/PAUSEX/ENDEX
  – Exercise Rules of Engagement (EXROE)

• Communications
  – Primary and backup communication channels
Documentation

- Scenario Mapping
- MSEL
- Playbooks
- Instructor/facilitation guides
- Range infrastructure
- Exercise environment configuration
- Data handling procedures
- ... many, many more
Lessons Learned

• Effective process improvement completes the exercise cycle

• After Action Review
  – Drive organizational change
  – Improve the exercise experience
Misc Cyber Exercises

• Notable cyber exercises
  – Cyber Storm (DHS NCSD)
  – Cyber Flag (USCYBERCOM)
  – Cyber Guard (USCYBERCOM, NGB, DHS, FBI)
  – Cyber Defense Exercise (DOD, Service Academies)
  – CyberPatriot (AFA)
  – Cyber Shield (NGB)
  – Bulwark Defender (USSTRATCOM)
  – …

• Cyber training and exercise service providers
  – Online competitions
  – Challenges
Demo
Summary

- Cyber exercises enable experience building in a controlled environment
- Effective planning is critical to the success of the exercise
- HSEEP provides a framework for designing cyber exercises based on best practices and a proven methodology
References

CERT® Approach to Cybersecurity Workforce Development
http://www.sei.cmu.edu/reports/10tr045.pdf

Chairman of the Joint Chiefs of Staff Manual 3500.03D – Joint Training Manual for the Armed Forces of the United States
http://www.dtic.mil/doctrine/training/cjsm3500_03d.pdf

DHS Exercise and Evaluation Program (HSEEP)
https://www.llis.dhs.gov/hseep

Methods for Enhanced Cyber Exercises
https://www.llis.dhs.gov/sites/default/files/Methods%20for%20Enhanced%20Cyber%20Exercises.pdf
Questions

Greg Longo
Cyber Workforce Development
U.S. Army Exercise Portfolio Manager
ggl@cert.org
412-268-8330