Mission Based Cyber Risk Assessments (MBCRA)

Lesson and all discussions are UNCLASSIFIED!

Briefs & References can be found at:
https://www.milsuite.mil/book/groups/cyberacq
https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Caution-Home.aspx
Cyber Risk Assessments

Cyber Risk Assessment Menu

• Many choices available – differ in methodology, ease of use, level of rigor, and end product

• Some factors to consider
  • Focus: system risk vs mission risk?
  • Reproducible? Repeatable?
  • Tailorable? Scale-able?
  • Resources Required (time, effort, cost)
  • Model-driven? SME-driven?
  • Threat knowledge required? Other data needs?
  • Validated? Peer-reviewed?
  • Level of experience required?
  • Developed by: government? UARC? FFRDC?

*Comparison of Cybersecurity Risk Methodologies
Rhiannon Hutton, Institute for Defense Analyses
rhutton@ida.org
Category – Methodology Mapping

Control-Focused:
- SCA-V TTP
- CIAM
- STPA

Risk-Only:
- CVRA
- LCRIT

Collaborative:
- OCTAVE
- CTT
- BlueBook
- TMCRA
- CRA SWP
- CSRA

Capabilities-Based:
- CJA + TARA
- BluGen
- MORDA

Modeling for Simulation:
- NMA
- MIRA
- MAAP
- MAAP
- CyMRisk
Each MBCRA Category Has Strengths and Weaknesses

- Time/$ investment required
- Expertise required
- Information available
- Inherent assumptions (uncertainty)

**Collaborative**

Uncertainty in attack selection and vulnerability identification
Depends on knowledge in the room and mission/system scoping

**Capabilities-Based**

Uncertainty in threat characterization
Depends on accurate knowledge (or prediction) of attacker capabilities

**Modeling for Simulation**

Uncertainty in model representation
Accuracy of simulation results depends on fidelity of underlying models
NETCOM Operational Risk Assessment

- IDA reports SCA-V-TTP risk method “Security Control Focused“ whereas the CTT / CRA would be more "Collaborative“

- Strongly linked to STIGs, CCIs and scans

- Numerical Vulnerability = (Severity x Impact x Countermeasure) / 10

- Modifies NIST 800-30/39 Risk Tables by
  - Aggregate Risk
    - If > 12 non-compliant controls & > 1/3 at high watermark level, aggregate risk increases

A consistent control focused process
MBCRA in the Cyber T&E Process

Six phases of cyber T&E*

- Phase 1: Understand Cybersecurity Requirements
- Phase 2: Characterize the Cyber Attack Surface
- Phase 3: Cooperative Vulnerability Identification
- Phase 4: Adversarial Cybersecurity DT&E
- Phase 5: Cooperative Vulnerability and Penetration Assessment
- Phase 6: Adversarial Assessment

Cyber Table Top Exercises inform Design, DT&E and ATO

Cyber Table Top Exercises inform response to change in threat or environment

*Reference: DoD Cybersecurity T&E Guidebook
MBCRAs: A Part of the Larger Cybersecurity Effort

- Supply Chain Risk Management
- Architecture Analysis
- Criticality Analysis
- Requirements Analysis
- MBCRAs
- Cyber portion of the Developmental Evaluation Framework
- Risk Management Framework
- Adversarial Cyber DT
- Cooperative Vulnerability Identification
- Attack Path Analysis
- Threat Assessment
- Adversarial Assessment

Cleared for open publication 23 July 2016, CASE # 18-51642 Department of Defense Office of Prepublication and Security Review
What is a Cyber Table Top?

• Lightweight, low cost, **intellectually intensive** wargame exercise
  – Verbal execution – no actual cyber attacks on systems
• Introduce and explore *through dialogue* the **effects of cyber offensive operations** on the capability of systems to continue to carry out or support military missions
• Two-sided wargame **focusing on two opposing missions**
• Provide program managers, engineers, and testers with **actionable information** on cyber threats to mission execution
  – Risks tied to mission impact as assessed by operational experts
    • Testing priorities
    • Mitigation priorities

CTTs identify risks that the Risk Management Framework (RMF) does not typically identify – and CTTs can assist with RMF risk assessment reporting requirements for RMF identified findings
Goals and value-proposition of the CTT

- **Pragmatic, affordable method** to implement elements of the DT/OT six cybersecurity phases
- **Generate actionable information** on high priority/high mission impact cyber threats
  - Inform analysis for the system survivability Key Performance Parameter (KPP)
- **Define specific high-value follow-on analysis and testing** to verify and quantify actual risks
- Provide the Program Manager’s engineering and test team **opportunities for risk reduction throughout the life cycle**
- **Reduce the likelihood and cost of cyber vulnerability discovery** during operational testing and deployment
- **Socialize the concepts of cybersecurity** for program office and operators, bridging the gaps between systems engineering, testing, and operating

CTTs identify risks that the Risk Management Framework (RMF) does not typically identify – and CTTs can assist with RMF risk assessment reporting requirements for RMF identified findings
Cyber Table Top (CTT)

System Familiarization
- Provide an overview of the supporting mission and capability gap integration that the SUT fulfills.
- Conduct a system level description of the SUT and associated modifications under test with a focus on communications, interfacing and integrated networks.
- Describe other supporting systems (e.g. maintenance laptops) and processes.
- Address multiple operator-level use case scenarios under varying conditions (e.g. initial vs. persistent deployment).
- Describe the operational environment(s) and associated security conditions.

Define Potential Threat Vectors
- Review prior documented test results.
- Obtain intel awareness of potential threats.
- Define potential threat vectors and decompose into Access, Escalation/Persistence, and Effect.
- Estimate “probability gates” of threat vector occurrence—based on specific operational conditions.
- Identify vectors where uncertainty is high and develop test strategies to reduce that uncertainty.
- Outline general resource and support requirements to accomplish the most effective assessment.
The Four Step CTT Process

1. Planning
   - Select leads & team members
   - Define mission & scenario
   - Collect & distribute reconnaissance
   - Generate candidate attack vectors

2. Knowledge Elicitation
   - War Gaming Seminar
     - Teams complete planning & brief participants
     - Working meetings & discussions to evaluate various attacks

3. Normalization & Analysis
   - Working Meetings
     - Extract key data from seminar notes & populate analysis table
     - Fill in gaps
     - Document likelihood, & impact of cyber attacks

4. Risk Synthesis & Recommendations
   - Working Meetings
     - Categorize attacks
     - Consider existing / possible mitigation
     - Develop risk matrices & recommendations
     - Brief out technical results & recommendations
     - Schedule leadership brief

The CTT process bridges “Mission Assurance” to “Risks from Cyber Threats” through proven, disciplined war-gaming methods.
Exercise Execution & Analysis

Establish:
- Purpose
- Goals
- Expected output
- Team missions

Present:
- Operational Team brief
- OPFOR Mission brief
- System under evaluation brief

Team Breakouts

Exercise Execution

Day 1
- Develop Mission Plan

Day 2
- OPFOR Attack Mission #1 - #N
- Operational Team describes mission impact and workarounds to the attack
- Both teams describe possible outcomes and system effects

Day 3
- OPFOR Team describes broad class of attack and goals
- Iterate with next broad class of attacks

Data collection and review

Analysis Participants

Document:
- Discussions, clarifications
- Data review and verification
- Follow on actions for SMEs
- Lessons learned, feedback

Cleared for open publication 23 July 2018, CASE # 18-S-1842
Department of Defense Office of Prepublication and Security Review
Plan ahead for Post Exercise Analysis

Key Products

- Analysis table documents attacks

- Risk matrices

---

Exercise Execution

Post Exercise Analysis
Plan Ahead for Impact & Likelihood Method

Operational / OPFOR Teams may begin to develop during breakout & during the CTT Execution
The final methodology is refined & finalized during analysis

<table>
<thead>
<tr>
<th>Impact</th>
<th>Mission Impact</th>
<th>Data Loss</th>
<th>System Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fully Mission Capable</td>
<td>No data compromised</td>
<td>System Performance Not Impacted</td>
</tr>
<tr>
<td>2</td>
<td>Partial to Fully Mission Capable</td>
<td>Public Access Level</td>
<td>System Performance Marginally Impacted</td>
</tr>
<tr>
<td>3</td>
<td>Partially Mission Capable</td>
<td>FOUO</td>
<td>Partial Loss of Functionality</td>
</tr>
<tr>
<td>4</td>
<td>Non to Partially Mission Capable</td>
<td>FOUO/New Technology</td>
<td>Major Loss of Functionality</td>
</tr>
<tr>
<td>5</td>
<td>Non-Mission Capable</td>
<td>Classified</td>
<td>System Performance Severely Impacted/Total Loss of Functionality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack Cost/Level of Effort</th>
<th>Nearly anyone can build: Nascent – Limited threat</th>
<th>Low cost to develop</th>
<th>Exists today</th>
<th>Easy to develop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Criminal level organization can build: Moderate threat</td>
<td>Medium cost to develop</td>
<td>Many can develop</td>
<td>Hard to develop</td>
</tr>
<tr>
<td></td>
<td>Nation state organization can build: Advanced threat</td>
<td>High cost to develop</td>
<td>Few can develop</td>
<td></td>
</tr>
</tbody>
</table>

Exercise Execution
Post Exercise Analysis
• **Access and Pivot**: Insert a cyber weapon/payload onto a computing system and move weapons between connected systems

• **Command and Control (C2)**: Trigger the cyber weapon within the system

• **Effect and Exfiltrate**: Generate system effects to impact system or human behavior disrupting the video or platform
Apply critical thinking

Think like a hacker

System Security Engineering Solutions

Wheel of Access A.K.A. Wheel of Doom

Prevent, Mitigate, Recover/Resiliency
Red Team (Adversarial / OPFOR) vs Blue Team (Cooperative / Operational / Hunt / Defender)

Red Team Portrays APT
- Recon
- Weaponize
- Deliver
- Exploit
- Control
- Execute
- Maintain

Advanced Persistent Threat Objectives
- Exfiltrate data
- Violate data availability
- Corrupt data integrity

Data Collection
- Attacker actions
- Defender detections
- Defender actions
- Mission activity

Defenders attempt to analyze attacks and determine courses of action

Blue Team Portray Test Items
- Detect
- Deny
- Disrupt
- Degrade
- Deceive
- Destroy
- Recover

Defender Objectives
- Protect Against Intrusions
- Detect Intrusions
- React to Intrusions
- Mitigate Intrusions
- Determine Responses
- Restore After intrusion

Source: Institute for Defense Analysis (IDA), developed for the DASD DT&E InterTEC Cyber Event (ICE) February 2013
“Red vs Blue Teaming” is a Way of Life

Simian Army

- Kill/inspect running instances
  - Chaos Monkey
  - Janitor Monkey
  - Security Monkey
  - Conformity Monkey
  - Chaos Gorilla*
  - Chaos Kong*

https://github.com/Netflix/SimianArmy
https://github.com/Netflix/security_monkey

Chaos Monkey randomly terminates virtual machine instances and containers that run inside of your production environment. Exposing engineers to failures more frequently incentivizes them to build resilient services.
CTT Facilitator Collaboration Site

https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/

Register on Intelink by going to the link and using a CAC (Instructions also in your Student Syllabus)

Do not click on files to open because you will edit the file – download (right-click) to computer and then edit; you can upload files too

Earn Certificate after you attend a CTT

Find a Facilitator

Ask a question

Find example files – Click on CTT Facilitators folder, right click to download files

Share best practices

Survey the program

Publish a CTT – find a CTT

Cleared for open publication 23 July 2018, CASE # 18-S-1842

Department of Defense Office of Prepublication and Security Review
CTT Facilitator Training Path

- Attend CTT Facilitator one-day training
- Attend a CTT as a participant, observer, or note taker
- Co-facilitate your first CTT with an experienced CTT facilitator

Provide feedback on the process: Complete Survey on Intelink

Certified!

Strongly recommend completing entire Training Path before conducting a CTT – observing/co-facilitating with an experienced facilitator is an invaluable step.
Questions?