Cybersecurity Test and Evaluation (T&E)

Top 10 Best Practices

March 2018
Prepared for:
5th Cybersecurity Workshop
Challenges Facing Test and Evaluation
Prepared by
Peter H. Christensen
pchris@mitre.org
703 983 2516

Approved for Public Release;
Distribution Unlimited. Public Release Case Number 18-3503
What, Why, How?

- **What do we want to accomplish?**
  - Help advance the state of the art of Cyberspace T&E

- **Why is this important?**
  - Cybersecurity T&E produces actionable information to improve Cyber Resiliency of Acquisition Programs

- **How will we do it?**
  - Provide some background regarding Cybersecurity T&E
  - Share best practices preparing for and executing cybersecurity T&E and provisioning cybersecurity T&E infrastructure
In 1957 Cybersecurity Testing was Easy!

1957 Porsche 356 Classic
Zero SLOC...No Microcontrollers!

“In Modern Automobiles There Are Over 100 Million SLOC Used By 70 To 100 Microcontrollers!”

Source: Protecting Our Future: Educating a Cybersecurity Workforce Vol 2

In 2018 Cybersecurity Testing is Much More Challenging!

Attack Surface: A System’s Exposure To Reachable And Exploitable Cyber Vulnerabilities Within The System Boundaries!

SANS Attack Surface Problem: http://www.sans.edu/research/security-laboratory/article/did-attack-surface
"Technical Debt": The cost of work that must be accomplished before a job is completed
- Type 1 Debt: incurred unintentionally
  - Flawed design or implementation
- Type 2 Debt: incurred intentionally
  - Decision to optimize for the present

DOD Cybersecurity sources of created “technical debt”
- Type 1: Cybersecurity Requirements
  - Constrained by “System Boundary” and focused on “Controls Verification”
- Type 2: Cybersecurity Testing
  - Constrained by venue or resources
  - Deferred until system has matured
Cybersecurity Testing Lessons Learned

1. Cybersecurity Testing is iterative and incremental throughout the acquisition lifecycle including O&S
2. Multidisciplinary, collaborative approach essential to optimize test planning
3. Effective Test Teams Understand The Adversary
4. Cyber Table Top (CTT) exercises help scope testing and understand mission risk
5. Iterative Risk Management Framework (RMF) and Cybersecurity Testing informs survivability and resiliency in a mission context
6. Start small and grow
7. Execute Cybersecurity Testing with Key IT Staff, Incident Responders and Cyber Protection Teams
8. Customers Require Cybersecurity T&E “As A Service” and “High Fidelity” T&E Infrastructure
9. Investments in multipurposed T&E infrastructure help programs keep pace with adversary, speed development and promote innovation!
10. Connectivity makes range/infrastructure location irrelevant!

Lessons Learned Come From Executing Testing And Training Events Over Last 14 Years!
Lesson Learned #1: Cybersecurity Testing is Iterative and Incremental Throughout the Acquisition Lifecycle

- Phases are iterative and incremental!
  - Initial phases reduce Type 1 Debt!
    - Complements System Security Engineering (SSE) and Risk Management Framework RMF activities
  - Later phases reduce Type 2 Debt!
    - Promotes understanding of mission risk!

Early T&E Engagement And Iterative Cybersecurity T&E Reduces Technical Debt Results Can Be Used To Inform Cyberspace Wargaming & Analytics!
Lesson Learned #2: Multidisciplinary, Collaborative Approach Essential to Optimize Test Planning

- All Stakeholders Must Actively Participate in Planning, Event Design, Execution
  - Capabilities Development, Program Management, Contracting, Systems Security Engineering, Risk Management Framework and Cybersecurity T&E, Cyber Defense and Offense

- Test By One Use By All!

Inform Cyberspace Wargaming & Analytics Must Include All Stakeholders Challenge: Finding Knowledgeable Cybersecurity Workforce!
Lesson Learned #3: Effective Test Teams Understand the Adversary

- **Cyber Attack Lifecycle**
  - Framework to understand and anticipate the moves of cyber adversaries at each stage of an attack.

- **Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)**
  - Adversary model and framework for describing the actions an adversary may take
  - Useful characterize and describe post-compromise adversary behavior

**Know Your Enemy….Think Like The Adversary!**
Lesson Learned #4: Cyber Table Top (CTT) Exercises Help Scope Testing and Understand Mission Risk

- **What is a Cyber Table Top Exercise?**
  - Low technology, low cost, intellectually intensive wargame
  - Introduces and explores the offensive cyber effects on operations
  - Assess system, SOS or FOS mission risk

- **Why is it used?**
  - **Identify** potential threat vectors, risks associated with threat vectors, and potential threats from boundary systems
  - **Categorize** cyber threat consequence by likelihood and impact within the assessed mission context
  - **Inform** mitigations analysis, engineering, testing and design activities

- **What does it produce?**
  - Cybersecurity risk matrices based on potential mission effects
  - Recommendations for actionable steps to increase resistance and resilience to cyber attacks

CTTs Are a Low Cost Cyberspace Wargaming & Analytics Tool!
Lesson Learned #4: Example: Family of Systems Cyber Table Top

Mission Focused
Family of Systems
Cyber Table Top

Informs Cyber Testing

CTTs Techniques Can Be Used for Wargaming!

Land
Sea
Air

Modified Graphics from: WIKIPEDIA Commons
Lesson Learned #5: Iterative RMF and Cybersecurity Testing Informs Survivability and Resiliency in a Mission Context

Iterative testing improves defensive capability

Include Defensive Cyberspace Assessments (DoDI 8530.01)

Vulnerability Assessment Teams
Threats Portray Attacks
Weaknesses/Vulnerabilities
Operational Administrative Technical Protection Mechanisms
System Capabilities Affected
Mission Consequences And Impacts

Vulnerability Assessment
Threats Portray Attacks
Weaknesses/Vulnerabilities
Operational Administrative Technical Protection Mechanisms
System Capabilities Affected
Mission Consequences And Impacts

Modified Graphic from: WIKIPEDIA Commons

RMF Necessary to Manage Program Risk.
DT&E, OT&E and Cyberspace Wargaming Necessary to Understand Survivability and Resiliency
The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

©2018 The MITRE Corporation. ALL RIGHTS RESERVED

OUUSD R&E, DD (DT&E) Cybersecurity Developmental Testing Phases 3&4
Evaluate Compliance, Cyber Survivability and Operational Resiliency

PHASE 3 TEST EVENTS
- RMF
- Interoperability Standards
  - NR KPP Certification
  - COMSEC
  - TEMPEST Certification
  - NSA Certification
  - STIG Compliance/ SRGs
- Configuration Guides
- Workforce Requirements

PHASE 3 & 4 Testing
- Interoperability Standards
- Cyberspace Defense IAW DODI 8530.01 & ESM v9.2
  - (I)PDRR

PHASE 3 & 4 Testing
Performance:
- CSA 1 Access Control
- CSA 2 (Not a beacon)
- CSA 3 (TRANSEC/COMSEC)
- CSA 4 (Protect system's information)
- CSA 5 (Critical Function Partitioning)
- CSA 6 (Minimize & Harden Attack Surface)
- CSA 7 (Detect anomalies)
- CSA 8 (Manage system performance if degraded)
- CSA 9 (Recover)
- CSA 10 (Actively manage system’s configs)

System Cyber Survivability
Ability to prevent, mitigate and recover from cyber attacks

Operational Resiliency
- Trustworthy information resources
- Ready for degradation or loss
- Operations have the means to prevail
- Mission focused – not system focused

PHASE 3 & 4 Testing
- Interoperability Standards
- Cyberspace Defense IAW DODI 8530.01 & ESM v9.2
  - (I)PDRR

PHASE 4 Testing
Operational Resilience:
- PDRR
- COOP
- Preserve TRANSEC
- Use of Automation

(I)PDRR=Identify, Protect Detect React, Restore
Underlined areas addressed as policy under DODI 8500.1

Source: OUSD R&E, DD (DT&E) Ms Sarah Standard, Cybersecurity Interoperability Technical Director
Lesson Learned #6: Start Small and Grow!

Focus on Systems of Systems Inter-Dependencies and Mission Risks

- What systems post the most significant risk to mission?

How? Decompose Systems of Systems (SOS) into subsystems

1. Identify key external connections that enable adversary “access” to mission critical paths
2. Identify the networks/subsystems that allow adversary to “pivot” to affect mission critical tasks
3. Cybersecurity DT&E – Contractor and Government testing
   - Cooperative Vulnerability Identification – start early
   - Adversarial Assessments: Take the system to failure in DT
4. Cybersecurity OT&E
   - Red Teams access and then pivot to create effects!
   - Involve Network Defenders, Cybersecurity Service Providers (CSP), Information Technology Workforce, etc.

Large Platforms Using This Strategy To Integrate Cybersecurity DT&E and OT&E
Lesson Learned #6: Example “Large Platform” Enterprise Test Strategy (Cont.)

- Large Platforms have extremely large “Attack Surface”
  - Adversaries access systems, pivot and create effects

- Example CVN Systems and Networks
  - Control Systems
  - Tactical Networks
  - Weapons Systems
  - Aviation Systems

- DT&E Key Question: Can an adversary create effects?
  - Test Venue: Labs, SILS and Ranges
  - VV&A ensures Test Data re-useable

- OT&E Key Questions: Can adversary pivot to system? Can Operators sustain mission?
  - Test Venue: Live on platform

Developmental Testing
Advanced Arresting Gear HITL

Operational Testing
Advanced Arresting Gear Installed

Modified Graphics from: WIKIPEDIA Commons
LL #7: Execute Cybersecurity Testing with Key IT Staff, Incident Responders and Cyber Protection Teams

- Operators, IT Staff, Incident Responders, Cybersecurity Providers (CSSP) and Cyber Protection Teams (CPTs) should be involved in testing!
- Defenders demonstrate and learn CONOPS to protect, detect, restore and recover!

Wargaming Team Must Include Knowledgeable Cyber Operators
Lesson Learned #8: Customers Require Cybersecurity T&E “As A Service” and “High Fidelity” T&E Infrastructure

- Customers typically “Wanted to do some Cybersecurity testing”
  - Unsure about scope, scale or fidelity
- Most Customers needed full spectrum Cybersecurity T&E Services
  - Event design, planning, Instrumentation, execution, post event data analysis and results reporting
  - Vulnerability and Adversarial Assessments
- “High Fidelity” Test Environment needed
  - May include legacy and new Hardware and Software Components
  - Complex network enclaves, enterprise, DNS/ISP services, traffic generation

Customers Needed Support Across Acquisition Lifecycle!

Example: IOT Network

High Percentage of Cyber Range Customers Required Full Spectrum Support!
Lesson Learned #9: Investments in Multipurposed T&E Infrastructure Help Programs Keep Pace with Adversary, Speed Development and Promote Innovation!

- Investing in “High Fidelity” Test Infrastructure has many benefits
  - Enables Agile Methods and DEVOPS
  - Improves efficiency and “Delivery Velocity”
  - Enhances Cybersecurity Posture
  - Enables DOD to evolve with adversary
  - Reduces ownership costs

- Industry now provisioning “Digital Twins”
  - Digital replica of physical assets, processes and systems that can be multipurposed

- DOD is pursuing Managed Secure Cloud Pathfinder for the Defense Industrial Base (DIB)
  - Emerging capability that could evolve to host Software Factories, DEVSECOPS, Digital Twins etc.

Acquisition Programs Can Benefit from Multipurposed High Fidelity Infrastructure!
Lesson Learned #10: Connectivity Makes Range/Infrastructure Location Irrelevant!

- DOD provisions multipurposed test infrastructure for functional, interoperability and Cybersecurity testing

- MILS networks are provisioned to support Cybersecurity Testing and Training
  - Joint Staff J-7, TRMC

- DOD has demonstrated ability to support distributed testing and training
  - Major training exercises remotely supported 1000’s of users
  - Connected numerous logical ranges
  - 100’s of enclaves & subnets
  - Thousands of nodes
Closing Comments
How Can We Help Move DOD Forward?

- Adopt a Proactive Approach to Deal Emerging Cybersecurity Threats
  - Embrace Cyberspace as an Operational Domain
    - Understand Cyberspace Operations Concepts
  - Understand how the Adversary Exploits Our Systems
    - ATT&CK, NSA/CSS Technical Cyber Threat Framework
  - Expect the Adversary to Find New Exploitable Vulnerabilities
    - Design for Resiliency
  - Develop and Continuously Deliver “Functionally Correct” and “Secure” Systems over the entire Lifecycle
    - Digital Twins, Software Factories, DEVSECOPS
  - Test Continuously: Early and Often
    - CT/DT/OT
  - Evaluate Cyberspace Operations and Cyber Survivability
    - Operators, Administrators, IT, Cybersecurity Operations and Cyber Mission Forces!
Questions?

Peter H. Christensen
Pchris@mitre.org
703 983 2516