Crafting Effective Cyber Exercises

April 25, 2025

Eric Tolbert, ACRP, CC
Kansas Cybersecurity
Exercise & Training Officer

Agenda

- What is a Tabletop Exercise?
- Best Practices
- Crafting the Exercise
- Engaging Stakeholders
- After Action / Hotwash
- Problems and Pitfalls
- Summary

Discussion-Based Exercises

- Seminars - discussion-based exercises designed to orient participants to new or updated plans, policies, or procedures in a structured training environment.
- Workshops - discussion-based exercises used as a means of developing specific products, such as a draft plan or policy.
- Tabletop Exercises - facilitated analysis of an emergency situation in an informal, stress-free environment. There is minimal attempt at simulation in a tabletop exercise. Equipment is not used, resources are not deployed, and time pressures are not introduced.

Operations-Based Exercises

- Drills - a coordinated, supervised exercise activity, normally used to test a single specific operation or function. It can also be used to provide training with new equipment or to practice and maintain current skills.

- Functional exercise - a fully simulated interactive exercise that tests the capability of an organization to respond to a simulated event. It is like a full-scale exercise but does not include equipment or deployment of actual field resources. It simulates an incident in the most realistic manner possible short of moving resources to an actual site.

- Full-Scale - simulates a real event as closely as possible. It is a multi-agency, multi-jurisdictional, multi-discipline exercise designed to evaluate the operational capability of emergency management systems in a highly stressful environment that simulates actual response conditions. Requires the mobilization and actual movement of emergency personnel, equipment, and resources.

Best Practices

The gold standard for exercise development is the Homeland Security Exercise and Evaluation Program (HSEEP)

HSEEP is a whole-community based approach that can develop, execute, and evaluate exercises that address the preparedness priorities

Exercises are crafted on priorities that are informed by risk and capability assessments, findings, corrective actions from previous events, and external requirements.

Why is HSEEP Important?

Provides a Standardized Framework - Ensures exercises are structured, effective, and scalable.

Focuses on Capabilities and Objectives - Aligns exercises with organizational priorities for targeted improvement.

Encourages Whole Community Involvement - Brings together stakeholders to create a comprehensive response plan.

Supports Progressive Planning - Gradually increases complexity to refine capabilities over time.

Improves Preparedness Through Planning - Captures lessons learned and provides actionable improvement steps.

Aligns with National Preparedness Goals - Strengthens core capabilities outlined in the National Preparedness System.

HSEEP Resources

Homeland Security Exercise and Evaluation Program | FEMA.gov

IS-120 An Introduction to Exercises
IS-130 How to be an Exercise Evaluator
E0146 Homeland Security Exercise Evaluation Program Basic Course
E0131 Exercise Evaluation and Improvement Planning
E0050 Exercise Control and Simulation
E0139 Exercise Design and Development

Master Exercise Practitioner Program (MEPP)
E0132 Exercise Foundations, Program Management, Design and Development
E0133 Exercise Conduct, Evaluation and Improvement Planning
K0136 MEPP Capstone Presentation

Crafting the Exercise

Clarify Objectives and Outcomes

- Define the Objective for the Exercise
  - What are you testing? (policies, communications, etc.)
- Define clear goals that are realistic (although the participants may not be aware of the goals initially)
- Make sure the goals align with organizational priorities
- Some objectives might be regulatory, or compliance driven (try not to overemphasize these, try to include practical and actional improvement goals)

Crafting the Exercise, cont.

Assemble the Right Team

- Who is on the planning team?
  - Executives
  - IT
  - Department heads
  - SME (Subject Matter Experts)

- Remember that business and organizational processes drive the scenario. IT supports but unless it is a specifically IT scenario, they should not drive the process.

- If they will participate, they shouldn't be on the planning team

Crafting the Exercise, cont.

Design a Realistic Scenario

- Create an engaging scenario
- Make the scenario challenging and broad enough that there are chances for all participants to engage
- If specific gaps in policies or procedures exist craft the scenario to stress those areas to promote growth and improvement

Crafting the Exercise, cont.

Things to consider

- Validate and Assess existing response plans, this is a chance to identify problem areas.
- Examine Roles and Responsibilities, does everyone understand their role, identify gaps in delegation of authority or look for a “weak bench” (backups and alternates)
- Work on problem solving and critical incident decision-making skills.
- Foster communication between groups

Engaging the Stakeholders

- Foster a no-fault environment to encourage open discussion. Make sure that everyone understands this is a “safe environment”

- Guide the conversations to keep them productive but allow for exploration of ideas. Sometimes a great conversation will occur but beware of allowing things to spiral off topic.

- Encourage active participation from all participants. Consider differing communication styles. Some people are more introverted than others and may be slow to speak up in a group.

- Be aware of power dynamics in a group, sometimes people are reluctant to speak out if management is in the room.

After Action / Hotwash

Capture Insights and Lessons Learned
- Document key findings and gaps

Develop an After-Action Report (AAR)
- Define specific actional steps for improvement

Implement Corrective Actions
- Commit to following up on improvement tasks
- Assign specific tasks to specific individuals
- Assign a timeline for the task to be completed
- Review for task completion

Problems and Pitfalls

Don’t go too BIG!

Problems and Pitfalls, cont.

Lack of Realism

- Over-Simplified Scenarios – often the scenarios don't reflect the complexity of an actual cyber incident.
- No Hands-On Testing – Tabletops usually are discussion-based, so there is no testing of actual systems, tools or response capabilities
- Not targeting weaknesses – include things like insurance gaps, communications issues, decision authority, lack of personnel or skills.
- Not enough pain in the scenario to make decisions painful or requiring compromise.

Problems and Pitfalls, cont.

Poor Preparation

- Vague Objectives – without clear goals participants may be confused about what they are trying to achieve.
- Poor Scenario Development – the scenario may not align with the organization's most relevant risks or threats.
- Misaligned stakeholder expectations – scenario did not achieve expected results or decision processing.

Problems and Pitfalls, cont.

Limited Stakeholder Involvement

- Exclusion of Key Teams – If only IT or IT Security is involved other critical stakeholders are left out (e.g. Legal, HR, PR, Executive Leadership, Facilities, Physical Security, Accounting, Finance, Vendors, etc.)
- Low Engagement – participants may not understand the value of the exercise, or don't understand the benefit of participation.
- Unrealistic Timelines – because timelines are compressed participants may not experience the stress of an extended, drawn-out incident, including staffing pressures.

Problems and Pitfalls, cont.

Neglecting Follow-Up

- Lack of Actionable Feeback – insights or gaps in processes gained during the exercise and not translated into concrete improvements.
- Lack of Improvement – The same issues remain unaddressed in future exercises. You keep testing the same thing over and over with the same issues.

Problems and Pitfalls, cont.

Inadequate Consequences

- Limited Impact Assessment – failing to consider real-world consequences such as loss of reputation, customer impacts, regulatory problems, including fines, impact to employee morale, etc.
- Poor Adversary Emulation – failure to take into account how actual “bad actors” react when they are discovered. Often cyber incidents turn into “Whack-a-Mole” in trying to eradicate the attacker presence in your systems.

Problems and Pitfalls, cont.

Human Factors

- Behavioral Oversights – some people do not perform well under stress. Human error, poor decision-making, physical stress is not realistically incorporated into the scenario.
- Inadequate Training – do the participants have the skills and knowledge necessary to respond effectively? Are they familiar with organization policies, procedures and response plans? Do they know where they are?

Improving Effectiveness:

Develop realistic, customized scenarios.

Involve cross-functional teams and external stakeholders.

Incorporate technical components and adversary simulation.

Focus on actionable outcomes and continuous improvement.

Align the exercise with the organization's risk profile and objectives.

By addressing these limitations, organizations can make tabletop exercises more impactful and better prepare for real-world cyber incidents.

QUESTIONS?

Kansas

Incident Response Resources

Homeland Security Exercise and Evaluation Program (HSEEP)
https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

CISA Tabletop Exercises
https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

FEMA Preparedness Toolkit
https://preptoolkit.fema.gov/

Incident Response Resources, cont.

Transportation Security Administration Exercise Information System (EXIS)
https://exis.tsa.dhs.gov/default.aspx

Kansas Department of Education Tabletop Exercises
https://www.ksde.gov/Kansas-Safe-and-Secure-Schools/Training/Safety-Drills-Exercises-and-Information

Incident Response Resources, cont.

NIST Incident Response Lifecycle: This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.

CISA (Cybersecurity Infrastructure Security Agency) Free Services and Resources: a list of free services and tools provided by private and public sector organizations across the cyber community.

GMIS International : GMIS International is a professional IT association of worldwide government IT leaders dedicated to providing best practice solutions for initiatives by providing its members with enhanced professional development, training, conferences, awards and networking while offering leadership though advocacy, research and shared experiences.

National Incident Management System

- **IS-700 NIMS, an Introduction:** This independent study course introduces the NIMS concept. NIMS provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents.

- **ICS-100 Introduction to the Incident Command System:** This independent study course introduces ICS and provides the foundation for higher level ICS training. It describes the history, features and principles, and organizational structure of the system.

- **ICS-200 Basic Incident Command System for Initial Response:** This independent study course is designed to enable personnel to operate efficiently during an incident or event within the ICS. ICS-200 provides training and resources for personnel who are likely to assume a supervisory position within the ICS.

- **IS-800 National Response Framework (NRF), an Introduction:** The course introduces participants to the concepts and principles of the NRF.

https://training.fema.gov/nims/

Training Resources

Security Training

- CISA Secure Our World Campaign
- https://www.cisa.gov/about/regions

Online and In-Person Training

- **CISA** (Cybersecurity & Infrastructure Security Agency)

  https://www.cisa.gov
- **FEMA** (Federal Emergency Management Agency)

  https://training.fema.gov/emi

  https://training.fema.gov/nims

General Resources

https://www.ebit.ks.gov/divisions/information-security-office-kiso/resources

Resources, cont.

Government Emergency Telecommunications Service (GETS)

Wireless Priority Service (WPS)

https://www.cisa.gov/resources-tools/services/government-emergency-telecommunications-service-gets

Resources

Kansas Information Security Office (KISO)
CyberSecurity Collaboration and Preparedness (CSCP)

Website: https://www.ebit.ks.gov/divisions/cybercollaboration
Email: KISO.CyberCollaboration@ks.gov
Request for Services: https://forms.office.com/g/RBkkmhG7pG

- **Misc. Resources**
  - Answer questions about resources
  - General knowledge
  - Facilitate connections and knowledge transfer
- **Tabletop Exercises**
  - Can provide stock templates of cyber-related incidents
  - Can help facilitate TTX exercises as staff availability permits

Upcoming Events

May 13, 2025 TEEX AWR136 Developing Cybersecurity Resiliency for Everyone, 8am – 5pm, Independence, KS
https://my.teex.org/TeexPortal/Default.aspx?MO=mCourseCatalog&D=EC&C=AWR136&S=754

May 19th thru 22nd, 2025 Comprehensive Cybersecurity Defense, Topeka
https://forms.office.com/g/dFhYhhebnp

July 14thru 17th, 2025 Cybersecurity Proactive Defense, Topeka (CCD Class pre-req)
https://forms.office.com/g/eJ8nskx0B4

August 5th & 6th, 2025 MGT 465, Recovering from Cybersecurity Incidents, Wichita (sponsored by Sedgwick Co Emergency Management, Sedgwick County Extension Center) Course ID: 1127426
www.train.org/ks

Upcoming Events

August 18th thru 22nd, 2025 Kansas Cyber Plains Guardian Exercise Training
Wichita & Topeka (In-Person Only)
https://www.ebit.ks.gov/divisions/cybercollaboration

August 25th thru 29th, 2025 Kansas Cyber Plains Guardian Exercise
Wichita & Topeka (In-Person & Virtual)
https://www.ebit.ks.gov/divisions/cybercollaboration

How Did We Do?

Please help us improve our presentations by leaving feedback for today's Crafting an Effective Tabletop Presentation

https://forms.office.com/g/DVc4gj0snJ

Don’t practice until you get it right, practice until you never get it wrong…

Kansas