ASHPOOL Cyber Operations

Tabletop Exercise Facilitator Handbook

Introduction

Tabletop exercises are used to help organizations find weaknesses in their security and processes in the response to an incident. Different scenarios can be used to test a myriad of responses to those scenarios. These are mainly "discussion-based" exercises, and help highlight teamwork, business policy, readiness, and more [5]. Throughout these exercises individuals will be guided through them by a facilitator and other tabletop exercise team members.

Table of Contents

About this Handbook

This tabletop exercise facilitator handbook template is meant to be used to help facilitate and lead different cyber-related incident handling scenarios from within an organization. It is necessary to give facilitators the proper information to create a thorough exercise, which in turn enables proper discussions and objective-driven play during the exercise itself [2]. Only the facilitator and facilitation team should view this handbook.

Preparation Considerations

A tabletop exercise is extremely limited in its success by the preparation that is done for it. Having more organizations and individuals involved to create a realistic exercise in combination with having staff time set aside along with budgets created for the purpose of these exercises creates an environment for them to succeed [1]. Having a dedicated meeting space, budget, and more can all help. These are not necessary for a tabletop exercise to be useful to the staff, but they create an opportunity for much more knowledge to be gained. Technically speaking, if necessary, a tabletop exercise can be run from a local library conference room that is reserved for a few hours [1].

Depending on the scope and scale of the exercise, different items can be focused on to provide a better experience for those involved. If a budget is available, additional helpers can be brought on like scribes, facilitators, cybersecurity subject matter experts, and even a dedicated area for the exercise to take place [1]. When determining all these items, the audience that the exercise is intended for must be considered [1]. This will determine how portions of it are developed and intended to be performed. After the target audience has been identified, the goal of the exercise can is able to be designated.

Here is a brief example list of pre-exercise activities:

- RSVP list
- Exercise Planning
- Team Sorting
- Room and Tech Setup

- Logistics of the Exercise

Objectives

Identifying the objectives of the exercise is critical as it allows the exercise to be built properly, and then also enables post-exercise reflection to see if the objectives were met. Figuring the objectives out can depend on determining the core capabilities of the needs of the team performing the exercise [1]. This can be anything from things they are bad at and need practice for, or things their management wants them tested on. The minimum number of objectives expected is three, as most tabletop exercises last from half a day to a full day, and three objectives can be completed successfully within that time [1]. Exercises should be tailored in order to showcase the wants and needs of the business commissioning the exercise in the first place.

There are also items called “SMART” objectives that can help the commissioning body decide on their objectives. “SMART” stands for specific, measurable, achievable, relevant, and time-bound [1]. A specific objective needs to cover who, what when, where, and why. A measurable objective needs to have a way to that it can be measured, whether that be numerically or descriptively. These measures should provide information regarding the cost, quality, quantity, and more [1]. The main focus of measurable objectives is to have observable actions and outcomes [1].

Achievable objectives are ones that are within the control or influence of the individuals that are participating in the exercise. These individuals must have the resources available that allow them to achieve that objective. A relevant objective is one that is relevant to the mission that the commissioning body has and should reflect on that body’s goals with their participation in the exercise [1]. Lastly, a time-bound objective is one that has a timeframe which has been laid out and is considered reasonable for the exercise and other objectives. This reflects on not just the exercise overall, but the choice of the objectives within it.

Please use the table below to help identify objectives for this exercise:

Objective	Reasoning	Core Capability

[2, 6]

Teams and Stakeholders

There should be a team identified for the exercise to properly meet its objectives. The exercise leadership team is made up of an exercise director, lead designer, lead evaluator, and a logistics lead [1]. Individuals are allowed to hold multiple roles, or multiple individuals can be in a single position. This team is responsible for the entire tabletop exercise, from the designing phase to the execution phase. Within this team are individuals who might also be referred to as "facilitators", "evaluators", or potentially even "observers" depending upon their role [2].

Outside of this team are the players and observers. The players are the individuals who are actively participating in the exercise and the discussions within it. Within the exercise different scenarios will be presented. The players will discuss or respond to these scenarios with actions. The observers are not directly involved in the participation of the exercise [2]. These observers can have input on the responses of players to simulated situations within the exercise, as they may assist these players in the development of their response or action through questions or providing helpful information [2].

There is another team involved in this process, and it is known as the "facilitation team". The leadership team mentioned above is responsible for creating and staffing the facilitation team [1]. This new team will take charge of the facilitation of the exercise and lead the individuals through the exercises within it. During the exercise, notes will be taken, and discussions will be had. These notes are taken to help evaluate the exercise regarding whether the objectives were met or not, and on how the exercise was run [1].

Roles and Responsibilities

Leadership Team	
Exercise Director	
Lead Designer	
Lead Evaluator	
Logistics Lead	

[1]

Facilitation Team	
Lead Facilitator	
Co-Facilitator(s)	
Lead Evaluator	
Evaluator(s)	
Scribe	

[1]

Scenario Types(s)

Tabletop exercises can be used to simulate almost any scenario, and the scenario chosen is normally based on the commissioning body's objectives. Along with the objectives, the core capabilities that were chosen are being evaluated as well [1]. Here is an example list of valid cybersecurity scenarios that can be chosen [1, 3]:

- Ransomware Attack
- DDoS Attack
- Physical Theft of a Laptop in the Field
- Attack on Infrastructure Vendors
- Data Theft by Employee
- Cloud API Key being Compromised
- Phishing Email Received and Opened

Here is an example list of a few things normally being looked at during these scenario simulations [1]:

- Employee response
- Coordination across organizations and teams

- Preparedness levels

Guidelines and Structure

Every exercise should have general rules and guidelines that stay the same no matter what. These exercises are done in the spirit of learning, which is why the environment they are hosted in will be an open, low-stress, and no-fault one [2]. Many people can be involved in these exercises, and they can simulate high-stress scenarios, which is why differing viewpoints, disagreements, and more are expected to show up at times [2].

These exercises also do not reflect on the current rules, policies, etc. that the commissioning body may hold. These are general exercises done to allow individuals to gain experience in the area, and to create a discussion surrounding the potential options and solutions to the given scenarios. Issue identification in these scenarios is less valuable, and the individuals involved should focus more on actions [2].

Participants are also expected to be mentally and physically present during the exercise if it is hosted on-site, and their phones and laptops should be on silent or powered off [6]. Everyone participating should be allowed to contribute to the discussion, and those contributions should be relevant and professional [6]. Participants should not tear others down if they make a mistake, instead, help instructing them of the issue and potential viable solutions.

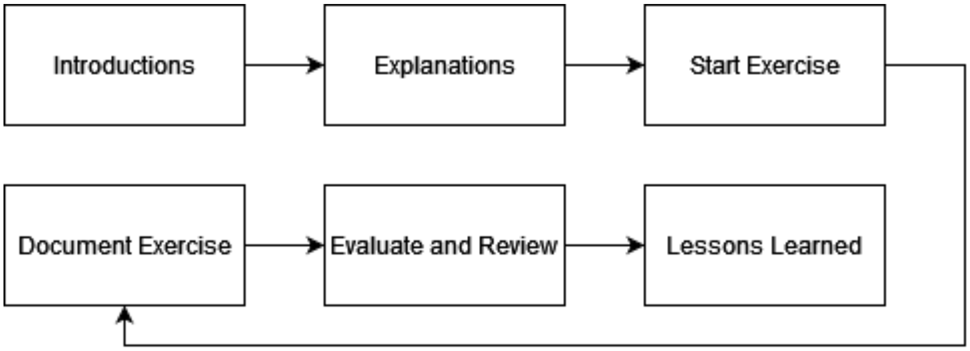
Exercise Module Template

Exercise Module Template	
Date	Time
00/00/0000	00:00 A.M. / P.M.
Exercise Name	
Exercise Details	
Scope	
Core Capabilities	
Relevant Locations	

Groups Involved	
Specific Objectives (Not Listed Above)	
Threat / Hazard	
Scenario Name	
Scenario Details and Impact	
Desired Outcome of Discussion	
Discussion Questions	Answers
Key Issues and Events	
Organizations Participating in the Exercise	
Timing of Engagement	
Targeted Participants	
Delivery Method	Online / On-Site
Sponsor	
Point of Contact	

[2, 4]

Exercises generally have a way that they are run once they begin. Here is an example:



[6]

Evaluating the Exercise

Evaluating an exercise is done using the original objectives created for it before the exercise occurred. In addition to that, it also considers the players' actions and discussions during the exercise, and what items they were able to achieve. Players can weigh in on the overall evaluation of the exercise through feedback forms [2]. All this information combined should allow the facilitator of the exercise to create a proper improvement plan [2].

Evaluation Form	
Was all the necessary information and resources present for you to fulfill your given responsibilities?	
Was the training you underwent or already have enough to support the response to the scenario?	
Did the exercise feel realistic?	
What worked and what didn't work during the exercise?	
Are you now sufficiently prepared to face a real-life scenario like the one simulated today?	
What changes would you make to this exercise?	

Rate the exercise over all out of ten.	

[3, 6]

Reflection

In the reflection phase, many different things can be looked at. Necessary changes can be found through reflecting on the exercise, the chosen scenarios, the participants feedback, and more [1, 2]. Improving performance, overall knowledge, discussion flow, comprehension, and the knowledge itself are all good goals to keep in mind when reflecting on these situations, as the evaluation and reflection phases can go hand-in-hand [1].

Record of Changes

Version #	Date Revised	Author	Revision Description
1.0	4/30/2022	Evan Read	Created the document.

References

[1] L. Costantini and A. Raffety, “Cybersecurity Tabletop Exercise Guide 1 | Cybersecurity Tabletop Exercise Guide Disclaimer,” 2021. Accessed: Apr. 30, 2022. [Online]. Available: https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

[2] State of Oregon Office of Emergency Management, “Facilitator Handbook,” *Oregon.gov*, 2022. https://www.oregon.gov/oem/Documents/EXPLAN_TEMPLATE.docx (accessed Apr. 30, 2022).

[3] University of Connecticut, “Tabletop Exercise Facilitator Guide,” *University of Connecticut Library*. https://s3.amazonaws.com/ultimatesdlc/UConnLib/Tabletop-Exercise-Facilitator-Guide.pdf (accessed Apr. 30, 2022).

[4] Mandiant, “Tabletop Exercise,” *Mandiant*, Sep. 2021. https://www.mandiant.com/sites/default/files/2021-09/ds-tabletop-exercise-000005-2.pdf (accessed Apr. 30, 2022).

[5] RoundTable Technology, “Tabletop Exercises: Scenarios to Help Prepare Your Cybersecurity Response,” *Pronto Marketing*. https://pronto-core-cdn.prontomarketing.com/2/wp-content/uploads/sites/1336/2021/01/RTT_eBook_TableTop-Exercises-rev2021.pdf (accessed Apr. 30, 2022).

[6] T. West, “(PDF) TABLETOP EXERCISE FACILITATOR HANDBOOK: Handling Instructions for Facilitators,” *ResearchGate*, May 2020. https://www.researchgate.net/publication/341115522_TABLETOP_EXERCISE_FACILITATOR_HANDBOOK_Handling_Instructions_for_Facilitators (accessed Apr. 30, 2022).

[7] FEMA, “National Cyber Exercise and Planning Program EMI-Virtual Tabletop Exercise (VTTX) Cybersecurity,” 2019. Accessed: Apr. 30, 2022. [Online]. Available: https://static1.squarespace.com/static/52e68c87e4b060b221fa9af5/t/5cfe868d2f658c0001847a2b

/1560184548792/FEMA+EMI+Cyber+VTTX+Situation+Manual+05202019_v00+%284%29.pdf

[8] CTS Security Operations Center, “Incident Response Planning The 15 Minute Workgroup Tabletop Exercise,” 2014. Accessed: Apr. 30, 2022. [Online]. Available: https://cybersecurity.wa.gov/sites/default/files/public/OCS_content/Trainingexercises/015%2015-Minute%20Workgroup%20Tabletop%20Exercise.pdf

[9] J. Kick, “Cyber Exercise Playbook,” 2014. Accessed: Apr. 30, 2022. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

[10] RedLegg, “Tabletop Exercise: Pretty Much Everything You Need to Know | RedLegg,” *RedLegg*. https://www.redlegg.com/solutions/advisory-services/tabletop-exercise-pretty-much-everything-you-need-to-know (accessed Apr. 30, 2022).

[11] K. Lake, “Implementing Your First Cybersecurity Tabletop Exercise,” *JumpCloud*, Oct. 26, 2021. https://jumpcloud.com/blog/implementing-first-cybersecurity-tabletop-exercise (accessed Apr. 30, 2022).