**Overview**

In order to have an effective Computer Security Incident Response Team (CSIRT) capability in any organization a plan must be in place. The plan is only effective if all members of the process are working together and understand their role. One way to ensure this happens is utilizing a table top exercise (TTX). A TTX is designed to incorporate a preplanned and fully scripted set of scenarios’ that test the current process flow. TTX are an easy way to train the entire team that would be involved in a real incident as well as identify areas for improvement.

The TTX will be a joint effort between the Crisis Prevention & Management team and the Information Security team. The ACME team will be basing the TTX off a set of industry best practices. Specifically, The “[Cyber Exercise Playbook](https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)” by Jason Lick of MITRE. The playbook provides an overview of the cyber exercise process from inception to reporting. Per the playbook ACME is choosing the Table Top exercise illustrated in the figure below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Style | Description | Complexity | Timing | Resources | Matches |
| Table Top | Paper-driven exercise with injects scripted by exercise planners and delivered via paper (cards/ discussion). | This type of exercise can be planned and executed quickly, depending on the number of organizations involved. | **Planning:** 1–2 months  **Execution:** 1–3 days | Limited resources needed, depending on number of organizations | Organizations new to exercises and to assessing organizational IA objectives.  Organizations that need to validate processes/ train personnel in-between other exercises. |

**Table Top Exercise Overview**

|  |  |
| --- | --- |
| Goal | Establish a baseline for future exercises; raise CSIRT awareness and skill. |
| Objectives | Clear, well defined goals: e.g., determine how Information Security staff interact and respond to an incident; validate procedures; observe and describe the process used to Identify, Protect, Detect, Respond, and Recover from simulated events. |
| Lesson Learned | Focus on what worked well and what requires improvement. |
| Future | Future exercises should enhance training by including live events. |

**Table Top Exercise Scenario**

* 3-hour session
* Tuesday, October 17, 2017 – Building X 8:00 am – 12:00 pm
* 1 scenario – The scenario will be a choose your own adventure exercise, with rewards (hints) for following the correct processes and procedures. The scenario will be easy at first to get the participants in the correct frame of mind. As the scenario progresses it will start to push the participants and possibly expose gaps in current people, process, and technology.

**Purpose**

* Practice incident response procedures related to Information Security in order to identify potential weaknesses in people, process, and technology.
* Educate and inform departments of the correct incident response procedures.

**Objectives**

* Expose and correct weaknesses in CSIRT processes and playbooks.
* Assess the effectiveness of CSIRT’s incident reporting and communication channels.
* Expose any gaps in data sources that could assist in the investigation.
* Determine the effectiveness of the various training given to the participants.
* Assess the participants’ ability to detect and react to threats during the exercise.
* Assess ACME’s guidelines for fixing issues (post-exercise).
* Enhance overall Information Security awareness and coordination.

**Participants**

* Information Security
* Crisis Prevention & Management
* Legal / Privacy
* Internal Audit
* Enterprise Risk Management
* Physical Security
* Strategic Communication
* Marketing
* Infrastructure & Operations

**Project Milestones**

* CSIRT Table Top Exercise Charter
* Training Room Reserved
* Participant List Developed
* High Level Draft of Scenario Finalized
* Flow chart of the Scenario
* Outline the scenario
* Build out WebApp for the scenario
* Get feedback about scenario
* Scenario Finalized
* Table Top Exercise Survey
* Evaluation document created
* Table Top Exercise Completed
* Table Top Exercise Feedback and Lessons Learned Documented
* Create a presentation to share internal / external