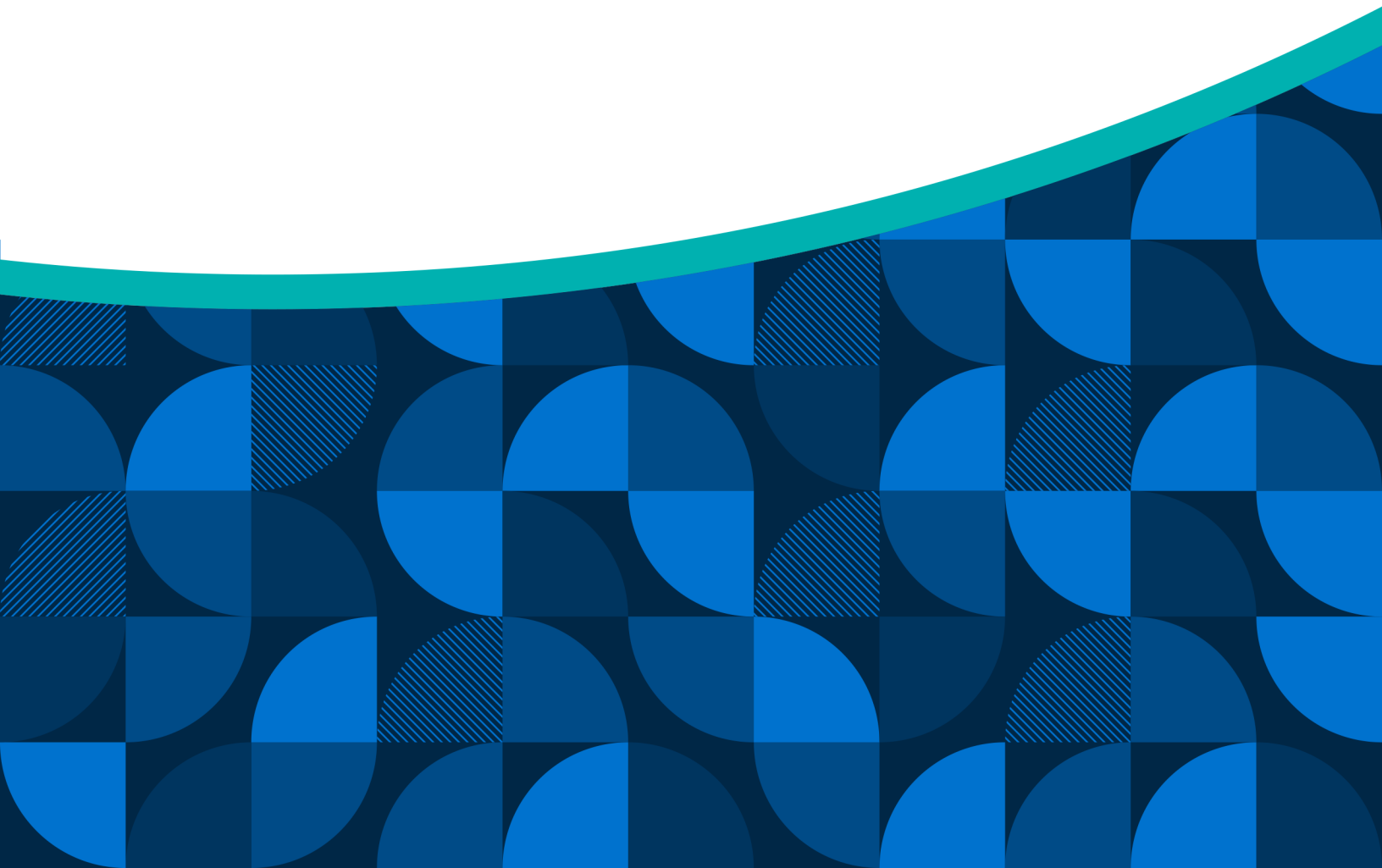
EAB

IT FORUM

Leading a Security Incident Response Tabletop Exercise

Guide for Facilitators and Observers



Abhilash Panthagani

Associate Director

APanthagani@eab.com

Kallie McGrath

Senior Research Analyst

KMcgGrath@eab.com

Table of Contents

Introduction

What are Tabletop Exercises?

Tabletop exercises allow IT/security teams and institutional leaders to simulate how they would react in the event of a complex short-term incident that requires a cross-functional and multidisciplinary response. Depending on the incident, they can be carried out by the IT/security team, president's cabinet, by a divisional leadership team, or by a curated set of relevant leaders both within and beyond the campus community. In response to the challenges our partners face when mobilizing their incident response, EAB has created a suite of materials that allow partners to implement tabletop exercises virtually.

Tabletop exercises are excellent tools because they require only a few hours of time and because they can be conducted by existing staff (i.e., not requiring a team of externally-contracted mediators). However, beyond the participants, two roles need to be filled: a facilitator and at least one observer. They should have the following traits:

- Ability to manage a conversation, listen carefully, interpret group dynamics, and offer insightful reflections
- Confidence in their standing with the leadership team that they can interrupt or redirect them comfortably or share candid observations about the quality of the dialogue
- Familiarity with the institution across multiple divisions

This facilitator role could be played by:

- Chief Information Officer
- Chief Information Security Officer
- President's Chief of Staff (if they do not have any formal role in incident response/emergency management)
- A trusted academic leader with widespread credibility
- An engaged and knowledgeable trustee
- A senior leader drawn from human resources, student affairs, institutional research, or another function that has broad view of the institution

Note: EAB experts may be able to fill these roles for you. Please reach out to your Strategic Leader if you are interested.

Phase One: Conducting the Exercise

Facilitation Instructions

Once a team agrees to conduct a tabletop exercise, the facilitator should study the EAB security incident prompt and create an agenda for how they will ideally move through the activity across the length of time allotted. Remember, the incident may have multiple stages. At least 90 minutes is required for a substantive exercise, though some may take several hours if they are especially complex or the group is highly engaged.

To begin the activity, participants should establish the following ground rules:

- Even though it feels odd, try to behave as though this is really happening
- You may not use your smartphone to call or text anyone on your team, or to research anything during this exercise
- You'll inevitably want more information than is provided, but you'll have to make do with what is available, planning for possible different contingencies, and stating your assumptions about what you believe to be true or what you do not know
- Thinking out loud can sometimes keep others from thinking clearly. Try to take notes and only speak when you're ready to share, unless the whole group is at a loss and you must all brainstorm together to generate possibilities
- Remember, a tabletop exercise is a "no-fault zone" where people can ask any question and admit uncertainty – it is a test of our plans, not of our leaders. There are no "hidden agendas" or trick questions in this exercise

Facilitation Tips

Allow participants to engage in back-and-forth without an intermediary. As a hands-off neutral moderator, you should let people chime in as they are inclined, even interrupting one another, as long as the conversation is generative and productive. However, if you sense participants are becoming overwhelmed, frustrated, or confused, consider pausing to synthesize what has been said so far.

Conflict is a valuable way to surface disagreements and try to resolve them. Interrupt conflict only if it becomes heated or if it becomes a conversation primarily between only two or three people. However, discourage participants from interrogating one another on their knowledge of obscure policies or subject-matter. If this begins to feel like a test of one leader or division, they will likely disengage.

The facilitator should pose questions and add interjections that add value to the dialogue. Vet if proposed solutions are realistic and not superficial…but remember, you do not have enough time to explore every line of inquiry all the way to its conclusion. Participants will get frustrated if you keep challenging their ideas and want every problem to exhaustion.

Sample Facilitator Contributions

Purpose	Sample Questions or Statements
Seek granular details that groups are inclined to breeze through	• So just to be clear, I heard that [XYZ] would need to occur, but I didn't hear who would be responsible for that. Could we clarify? • Let's pause for a second—you mentioned a campus-wide communication would go out, but what sort of content would it include?
Assess assumptions that are not clearly stated	• A few times so far, folks have referenced "resources" that we would make available to students or faculty in that event. But what "resources" are we talking about? Do they actually have the [equipment, training, curriculum] to do that? • OK, so we agreed we would purchase [XYZ]. Do we know which supplier or vendor we would use, if that is available right now, how much that would cost, or what account it would come out of?
Confirm a broad understanding of a technical or complex matter	• You referenced [a process/system/technical topic] that I'm not sure the rest of the group understood. Would you mind just explaining for a moment what you're talking about? • Can we pause to raise hands – how many could explain what *Terry* just said to all of their direct reports? [Seeing few hands] *Terry*, could you explain that again?
Identify reliance on individuals or resources	• *Alex*, you said you would handle media inquiries, but if you could not for some reason, who on your team would you deputize to do that? • What if in this case we were not able to get the Board of Trustees together for a few weeks?
Solicit participation from quiet members	• *Juanita*, we've been talking about staff for a while here. I know some of those are unionized. How much does what is being said here align with your understanding of the contract and relationship? • Can somebody chime in and share how they think that would be received from the faculty point of view? • *Shawn,* you've been quiet. What would your team want to add if they were here?
Affirm participants who take risks to suggest a counterintuitive perspective or acknowledge uncertainty	• Thanks for saying that. That's a good point. Just curious, who else would agree with that? • Roberta, I just heard Michael say that the greatest impact would be on [XYZ] kind of students. Do you see it the same way? Could I ask you to play devil's advocate on that for a moment and disagree?
Refocus the conversation when it goes in unproductive directions	• Dr. Gonzales, I think you've brought up a valuable point here about faculty workload, but I'm not just sure it's a topic we can do justice within this exercise. Can we set that aside and return to what I think Karen was asking about, with [XYZ]? • [After a period of silence while the group is grappling] OK, if we aren't sure what to do here, why don't we list possible options and the benefits and drawbacks of each? What could be the consequences of each approach?
Manage the flow of discussion	• I'm going to ask us to pick up the pace a bit. Let's fast forward through [a complex process we're currently discussing]. With just 10 minutes left to spend in this part, what are the final two to three things that would need to happen after that? • OK, I want to acknowledge we're all struggling on the media and communications component, but let's put a pin in that for now and at least see if we can address the financial implications in the next 10 minutes.

Observer's Guide

Observers, sometimes called evaluators, should take notes on the conversation as it unfolds. They are able to notice patterns or habits of thinking that are not evident to those participating in or facilitating the exercise. In addition to being able to take detailed notes, observers should be familiar with the members of the team, and comfortable enough to provide honest feedback on group dynamics, decision-making, and efficiency.

Here are some prompts to help them take rich notes that can provide substance to the debrief:

- Are there any topics, processes, or systems where the exercise team seems to have a particularly weak understanding?
- Where did the group move too quickly without ascertaining shared understanding or agreement?
- Were any assumptions made about the capability or readiness of various departments to take certain actions that should be investigated further? Were these assumptions clearly stated by the group?

Phase Two: Debriefing the Exercise

Facilitation Instructions

After the exercise ends, the facilitator should pose these questions:

- What worked well in this tabletop exercise?
- What did we seem to struggle with in this tabletop exercise? What might be our areas for improvement?
- What were the biggest discrepancies in our expectations or understandings?
- Why did we make a decision in a certain way?
- What other perspectives were not included that should be going forward? And how?
- What are the next steps we should take to remedy the problems that we surfaced during this exercise?

The group should be provided five to ten minutes to quietly reflect or take notes. They can choose to simply call on participants who want to speak, but to force contribution, they could also go around the table and ask participants to take turns responding to these prompts. After the participants debrief, the observer should be asked to supplement with their notes.

The facilitator or observer should help take notes on a white board or on a projected document that all the participants can see.

Sometimes, a debrief conversation is sufficient to identify clear takeaways and next steps. But institutions seeking to make the most of a tabletop will task their chief information officer, chief information security officer, chief of staff, senior incident response/emergency management leader, or another team member to prepare a formal after-action report with clear next steps and then request updates over time on the schedule of proposed corrective actions.

Use the accompanying EAB template to complete an after-action report with your team.