Cybersecurity Tabletop Exercise Tips

OVERVIEW

A tabletop exercise, or TTX, is a role-playing activity in which players respond to scenarios presented by one or more facilitators. Players usually play their own role of CEO, IT lead, or communications rep, but they can also play other roles to fill in gaps.

The facilitators will present some facts to the players that appear innocuous but may later turn out to have signaled a serious issue. They may provide information that seems contradictory to established facts, or that could cause the team to be distracted from the real problem.

The goal of the TTX isn't for all players to perform perfectly. The goal is to work as a team and to work out any problem areas in peacetime. There will be no opportunity to align the team in wartime.

ROLES

Organizations of different sizes can scale their TTX as appropriate. Typical roles in a TTX exercise include:

- **Players** (or participants) have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
- **Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

SOME SUGGESTIONS AND THOUGHTS

- Think out loud, like on game shows. Doing so also reduces any tension among players.
- Support each other. If someone is struggling, ask clarifying questions. Ask them who they would normally turn to for advice in a real crisis.
- Spot the gaps in your team. "No one is really in charge of that here" is a common observation, and one that might require action.
- If key people are not available to participate, you can use that in your scenario. For example, if the head of sales is not available for the exercise, the scenario could involve them being on an airplane and unreachable.
- All players should have a chance to participate. There should be no spectators, only participants. Facilitators can call on people to provide their assessment of the responses even if the current scenario does not formally include them.
- TTXs do not have to be large productions. You can supplement a full TTX exercise with a scaled down 10-minute discussion at the start of a staff meeting. For ideas, follow this twitter account: https://twitter.com/badthingsdaily
- Open a shared document, like in Google Docs or Microsoft SharePoint, so everyone can add notes. You can

have someone act as the Note-taker in that doc, but it's also helpful to have everyone add comments, questions, and suggestions for improvement in that document in real time.

- Have fun! While the topic and the need to rehearse is very serious, participants will learn and retain more if the atmosphere is friendly and supportive.

COMMON TTX MISTAKES

Here are some common mistakes teams make during a TTX exercise. Keep an out!

- Not having the printed Incident Response Plan (IRP) on hand, or not referencing it
- Forgetting to check to see if your printed contact list is current. Phone numbers change. Also, you'll often need to add people to it in light of a particular scenario.
- Assigning an Incident Manager (IM) too late in the game. Separating the Technical Lead functions from the IM functions can cost valuable time.
- Forgetting to notify key stakeholders, like investors, before the news articles show up
- Not notifying law enforcement, or having a non-lawyer notify them

After a TTX exercise, remember to incorporate your lessons into the Incident Response Plan (IRP) and other policy and procedure documents. For the TTX to be most effective, you will need to evolve your organization's habits and behaviors each time, even if in small ways.

EXAMPLE SCENARIO

Here is one example TTX scenario.

> Michael, a senior accountant, gets a call from the company's bank. The bank representative is confirming that they successfully transferred $50,000 to one of their existing vendor's new offshore accounts. However, the second payment of $150,00 failed because of insufficient funds. He wants to know how to proceed.
>
> Michael did not initiate either transfer, and he does not know about any offshore accounts for any of their vendors. He is the only person authorized to transfer funds.

What is your response?

SEE ALSO

- CISA guidance: https://www.cisa.gov/cisa-tabletop-exercises-packages
- CISA sample TTX exercises: https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team