SOPHOS

# How to Run a Cybersecurity Tabletop Exercise

**Best practices for using tabletop exercises to help your organization prepare for cyberattacks**

*A Sophos Whitepaper. July 2024*

# Introduction

Tabletop exercises test how well a team or process works by simulating a situation and acting out the planned response action. They have long been a valuable tool to prepare for adverse scenarios. The military runs tabletop exercises to experiment with different strategies in conflict situations while governments use them to improve response to crises. Within organizations, tabletop exercises are an effective way to prepare for cyberattacks.

This guide explains what security tabletop exercises are and how to run them. It is based on the approach that is used by the Sophos Cybersecurity team to prepare our own organization for an attack.

Transparency is a longstanding cornerstone of Sophos's philosophy, and we are pleased to share our strategies and resources. Visit our Trust Center for further insights and resources.

# What is a Tabletop Security Exercise?

A tabletop exercise encompasses a cyberattack and its potential damage. It enables you to see how well your organization will respond to an attack, and also provides you with cybersecurity insights to help you finesse your approach.

# Why Are They Important?

**Blind Spot Identification:** Security tabletop exercises help you identify cybersecurity blind spots before cybercriminals can find and exploit them.

**Security Posture Analysis:** With cybersecurity tabletop exercises, you can assess your security posture and find ways to optimize it.

**Communication Analysis:** Tabletop exercises for cybersecurity can highlight communication issues among teams or departments that can hamper your ability to address cyberattacks.

**Compliance:** Conducting and documenting tabletop exercises for security is an incident readiness requirement for security programs in many highly regulated industries.

**Response Fluency:** Walking through responses in a simulated incident enables participants to develop fluency with the actions needed in a real attack, accelerating execution.

# Types of Security Tabletop Exercises

There are several types of exercise, each taking different lengths of time and offering different benefits.

## Rapid-Fire Scenarios

A rapid-fire scenario is "extremely high level meant to be understood and discussed easily and quickly," according to ISACA. It requires little to no preparation and lasts about 10 to 30 minutes.

Rapid-fire scenarios can include junior-, mid-, and senior-level team members from a wide range of backgrounds. These team members can review multiple security scenarios, and each can serve as an incident responder.

## Technical-Only Scenarios

Technical-only scenarios typically last one to two hours. These scenarios promote in-depth technical discussions and require extensive planning. They allow team members to evaluate the technical aspects of a security incident.

A technical-only scenario usually involves a "seed" event. As the event unfolds, your organization can add more details to it. This can help team members prepare for complex cyberattacks.

## Full-Stakeholder Scenarios

Full-stakeholder scenarios are expansions of technical-only scenarios. They focus on technical issues and non-technical problems and logistics.

A full-stakeholder scenario generally lasts two to four hours. It can include technical team members along with legal, marketing, and HR professionals.

Full-stakeholder scenarios are ideal for organizations that want to improve communication between their teams or departments. It can be beneficial to include both technical and non-technical personnel in a full-stakeholder tabletop exercise. This gives participants from many teams or department the opportunity to work together to address a security issue.

Some organizations ask teams or departments to enter at different times during the scenario. This allows these teams or departments to become involved in the same way they would if a real-world security incident occurs.

# Who Runs a Tabletop Security Exercise?

Tabletop security exercises can be run by external or in-house teams, with both offering advantages to the organization.

## External

Third-party tabletop security service providers facilitate and manage scenarios and prompt discussions. They require little to no effort by you to set up and run.

The external provider will typically tailor the tabletop exercise to your specific organization and environment. Usually, they learn about your business and security challenges, and then develop a custom security tabletop exercise aligned to your situation.

## In-house

You can craft your own security exercises. While it can be costly and time intensive to develop and implement tabletops in-house, it does allow you to fully customize the cybersecurity exercises to your organization and environment. For example, these challenges can involve systems that participants use daily, making them more "real" and drive deeper engagement.

In-house tabletops also ensure participants can work together to identify and address specific issues that directly impact your organization, employees, and customers.

# The Sophos approach

At Sophos, we craft custom tabletop cybersecurity exercises for specific teams or departments. In an exercise, we usually start with a minor security issue and encourage participants to share their approaches and ideas with one another. From here, we use "findings" to highlight the severity of the issue.

Below are some of the cybersecurity scenario themes that we have run and that organizations can use to develop and run their own tabletop exercises.

| TEAM | SCENARIO |
|---|---|
| Sophos X-Ops | Insider threat |
| HR | Ransomware and employee PII leakage |
| Technical Support | Targeted attack by someone posing as a customer |
| Marketing | A compromised employee leading to the defacement of the company website and social media |
| Legal | Malicious bug bounty researcher |
| Sophos X-Ops | Compromised analyst system, supply chain attack |
| Engineering | Compromised Sophos binaries, supply chain attack |
| Engineering | Phished engineer |
| IT | Large-scale ransomware incident |
| Engineering | Zero-day vulnerability in application leading to compromise of customer base |

# Best Practices for Developing a Tabletop Security Exercise

The following best practices will help you get started with developing effective security tabletop exercises of your own:

## 1. Identify Your Target Audience

Determine your target audience, then develop your cybersecurity scenario. For instance, a complex security scenario is ideal if you are testing your cybersecurity team. Comparatively, if you are testing your IT or DevOps team, choose an issue that participants will understand and give the time, energy, and attention it deserves.

## 2. Choose the Right Participants

Decide whether to include a single team or department or multiple teams or departments in your security scenario. A single-team scenario lets you see how specific participants will respond to a cyberattack. Meanwhile, including several teams or departments encourages stakeholders across different business units to work together to address a security incident.

## 3. Figure Out When to Involve Participants

Consider when different teams or departments should be brought into your cybersecurity scenario. For example, if your organization's personally identifiable information (PII) is compromised, you may need to involve members of your legal team to ensure compliance with GDPR and other data security mandates.

It is often beneficial to include at least one person from every team or department within your organization in a security scenario. Doing so helps foster cross-functional communication and collaboration.

## 4. Decide How Many Participants to Include

Make sure your scenario includes participants who can engage with one another and work together to achieve common goals. In our scenarios, we often include up to 25 participants from multiple levels of a team or department or several teams or departments. Consider the size of your organization and structure of your teams and departments as you decide how many participants to include in your tabletop security exercises.

## 5. Manage the Time for Your Exercise

Give participants sufficient time to complete your tabletop exercise. At Sophos, we try to avoid lengthy tabletop exercise sessions. This is because it can be difficult for participants to coordinate their schedules and join a session that lasts more than a few hours.

## 6. Prepare Your Materials

Use a PowerPoint presentation or other materials to present your scenario. The Sophos team commonly uses PowerPoint presentations for tabletop exercises, with each slide showing a progression of events and questions for participants to consider. We usually limit the size of most of our PowerPoint presentations for these exercises to 20 slides.

## 7. Build Your Tabletop Story

Develop a theoretical story and tailor the information that you include in it accordingly. Recent news stories help get participants' attention. For large stories, you can put breadcrumbs in systems and logs for participants to find and follow.

## 8. Match Your Tabletop Exercise to Your Participants

Create a tabletop cybersecurity exercise based on the security maturity of your participants. For instance, a detailed story can be beneficial for participants with a wealth of cybersecurity skills and expertise. In other situations, a generic high-level scenario may work best.

If you develop a detailed narrative, make sure it is realistic. For example, if you want to target a specific part of your organization or network, get insights from someone into this area. Then, you can develop a scenario that resonates with your target audience.

## 9. Get Feedback from Participants

Ask participants if they have any ideas that you can incorporate into your exercise. Most participants can share insights into security pain points that they encounter on a daily basis. You can use these pain points to develop a scenario that helps participants find ways to address such issues moving forward.

## 10. Map Out Your Scenario

Craft a flow diagram of how your simulated attack could play out. This helps you find gaps in your story. Also request feedback from members of teams and departments who understand the issues addressed in your story. These team and department members can help you resolve any issues and ensure that your scenario is realistic.

## 11. Create Discussion Questions

Write down any questions that come up during the development of your story. These questions can prompt discussions among scenario participants.

## 12. Review Your Story

Evaluate your scenario multiple times before you present it to participants. It can be difficult to determine how long it will take participants to complete your story. When in doubt about the amount of time required, err on the side of caution. If you find your presentation runs close to or beyond the time available to participants, revise it as needed.

## 13. Set the Tone for Your Exercise

When participants arrive for your exercise, encourage everyone to participate whatever their level of seniority and tenure. The exercise gives each participant an opportunity to share their voice and help your organization improve its security posture. The more participants communicate and collaborate with each other, the more value everyone will gain from the exercise.

## 14. Moderate the Exercise

Moderation is important for keeping the exercise on time and track. However, the moderator should resist the urge to participate. In this role, you can provide participants with the scenario and help them move through it. You can also give participants time to discuss various story topics and share discussion questions and prompts.

## 15. Track Any Issues

Make sure that someone is taking notes about any issues that come up during the exercise. You can get insights into issues that otherwise hamper the effectiveness of your story.

## 16. Watch the Clock

Set a timer for your exercise and stick to it. Keep participants on track and remind them to continue to work on the story as it progresses.

## 17. Review Your Results

Following your tabletop exercise, consider the results and how they can be integrated into your organization's daily operations. For example, if you completed the test based on compliance mandates, you can create a PDF that contains the information that auditors need.

You can also give participants the opportunity to review your findings and run the same exercise at a later date. This can confirm if fixes or changes have helped you address any issues that were discovered during your initial exercise.

## Example Ransomware Tabletop Exercise

We are pleased to share a ransomware tabletop story that we wrote and ran at Sophos: Ransomware Tabletop.

You are welcome to use it directly or leverage it as the basis for developing your own stories.

## Tabletop Cybersecurity Resources

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) offers resources to help organizations conduct their own tabletop exercises. You can access more than 100 CISA Tabletop Exercises (CTEPs) designed to address a variety of threat scenarios, including:

- ✓ Cybersecurity: Consist of ransomware, insider threats, phishing, industrial control system (ICS) compromise, and other cybersecurity-based scenarios.
- ✓ Physical Security: Include active shooting, vehicle-ramming, improvised explosive devices (IED), unmanned aircraft system (UAS), and other physical security-based scenarios.
- ✓ Cyber-Physical Convergence: Focus on physical from threat vectors and cyber impacts from physical threat vectors.

Along with these, CISA offers pre-built templates that you can use to develop your own tabletop exercises.

## Conclusion

The proven effectiveness of tabletop exercises underscores their critical role in modern cybersecurity preparedness. As cyber threats become increasingly prevalent in the digital age, organizations must adopt and adapt these exercises to safeguard their operations. By understanding the fundamentals of security tabletop exercises and implementing the best practices outlined in the report, organizations can enhance their resilience against cyberattacks, ensuring they are well-prepared to face and mitigate them.

Sophos Trust Center - https://www.sophos.com/en-us/trust

Sophos Ransomware Tabletop - https://assets.sophos.com/X24WTUEQ/at/hvsj54g5zq5hhcfb3xrfnmk/sophos-ransomware-tabletop-exercise-overview.pdf

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

Transparency is central to Sophos's philosophy.
Explore our Trust Center for more insights and resources.:
www.sophos.com/trust



2024-07-24 (WP-DD)

SOPHOS