BLACK BEAR
ACADEMY

Table Top Exercise (TTX)

When a cyber incident occurs, company operations need the right processes, tools, and resources to respond and reduce business impact. The cybersecurity incident response lifecycle is the foundation on which all incident response and recovery activities are based.

A successful cyber incident impacts business operations, reputation, customer trust, and company profitability. In cyberspace, threats are evolving continuously, and the tactics, techniques, and procedures (TTPs) employed by the attackers are getting more sophisticated than ever. If an organization does not respond to a cybersecurity incident properly, there is a good chance that it would either experience the heavy penalties from regulators or take years to get back the customer trust.

This document serves as a guide to the participants of the table top exercise (TTX). Throughout the tabletop exercises, participants will be assessed on how well they responded to the cybersecurity incident scenarios throughout the incident lifecycle in relation to their documented plans, processes and procedures leveraging industry best practices.

What is a Table Top Exercise?

A Table Top Exercise (TTX) is a guided cyber incident which evaluates cyber incident processes, tools and shared services in responding to cyberattacks from both a corporate strategy and operational response perspective. We have introduced multiple scenario injects based on real world incidents in an online round table environment. The participants responses and actions are observed through 4 scenarios namely.

What do you get from the exercise?

During the initial phase of the tabletop exercise, our cyber incident consultant(s) develop an understanding of the organization’s workflow by understanding their cyber threat concerns, operational tools and internal processes. During the exercise proper, the cyber incident facilitator conducts an online discussion about the scenarios with key stakeholders and introduce the cybersecurity incidents with injects based on the modus operandi of attackers observed during our experience in the front lines. During the table top exercise, we observe the stakeholders to determine how simulated actions and decisions are made, concurrent to the current company’s documented plans, tools, and processes. After the exercise has concluded, the facilitator will brief the stakeholders after 1 week and submit a written After-Action Report that includes a step-by-step summary of scenario observations and responses.

Who should attend?

This exercise will be delivered and conducted through a series of videos, presentations and exercises:

Duration	1 day
Delivery Format	Facilitator interaction and online
Prerequisites	• Participants with basic knowledge on IT and incident operations • Participants with authority to make decisions
Requirements	• Web browser (preferably chrome for technical participants) • Zoom client (for participants)
Who should Attend	• Data Privacy Office representative • CIO or VP of Security & Control • Security Operations Center representative • IRT representative • CISO or CISG representative • Legal representative • Application Team (Web Application) representative • Helpdesk, Administrators, Network (Point of Contacts) • Audit IS representative • Corporate Communications representative

Detailed Table-Top Exercise Run Guide

Below is the proposed schedule of the exercise based on the agreed timeline during the initial preparation phase:

Time	Activity	Details
9:00 AM – 9:30 AM	Introduction & Objectives	- Overview of the exercise - Outline of roles and responsibilities - Set expectations for outcomes
9:30 AM – 10:30 AM	Scenario 1: Phishing Attack & Ransomware Infection	- A phishing email leads to a ransomware attack - Participants need to identify indicators of compromise (IoCs) and respond
10:30 AM – 11:00 AM	Break	
11:00 AM – 12:00 PM	Scenario 2: Insider Threat	- A disgruntled employee is suspected of data theft - Participants must detect, investigate, and mitigate the threat
12:00 PM – 1:00 PM	Lunch Break	
1:00 PM – 2:00 PM	Scenario 3: Business Email Compromise (BEC)	- Executive's email is compromised, and fraudulent wire transfers are attempted - Teams must respond by securing the email account and mitigating financial damage
2:00 PM – 3:00 PM	Scenario 4: DDoS Attack on Critical Services	- A Distributed Denial of Service (DDoS) attack targets the organization's web services - Participants will need to identify mitigation strategies to ensure uptime and prevent further attacks
3:00 PM – 3:30 PM	Break	
3:30 PM – 4:30 PM	Debriefing & Lessons Learned	- Discuss the results of each scenario - Identify gaps in incident response plans - Highlight best practices and areas for improvement
4:30 PM – 5:00 PM	Closing Remarks & Next Steps	- Summary of the exercise - Assign action items for improving future readiness

Scenario Details:

Scenario 1: Phishing Attack & Ransomware Infection

Situation: An employee opens a phishing email, leading to a ransomware infection on their system.

Objective: Identify the entry point of the ransomware, isolate the affected systems, restore services, and communicate with management.

Scenario 2: Insider Threat

Situation: A recently terminated employee is suspected of accessing sensitive company data and leaking it.

Objective: Monitor internal network traffic, identify the data exfiltration, and stop further damage.

Scenario 3: Business Email Compromise (BEC)

Situation: An executive’s email account has been compromised, and fraudulent wire transfers are initiated.

Objective: Secure the email account, notify the finance team, stop unauthorized transactions, and implement additional security controls.

Scenario 4: DDoS Attack on Critical Services

Situation: The company’s website and services are targeted by a large-scale DDoS attack, causing service disruption.

Objective: Implement incident response protocols to mitigate the attack, ensure service availability, and coordinate with external service providers.

Conclusion

Upon completion of the tabletop exercise, the participants will be able to:

1. Identify and Assess Cybersecurity Threats: Participants will have gained practical experience in recognizing various cybersecurity threats, including phishing, insider threats, business email compromise, DDoS attacks, and supply chain risks.
2. Enhance Incident Response Skills: Teams will improve their ability to follow incident response protocols, including threat detection, isolation, mitigation, and recovery procedures, ensuring rapid and effective responses to real-world cyber incidents.
3. Improve Communication and Collaboration: Through the exercise, participants will have learned how to communicate effectively across departments (IT, management, legal, etc.) and coordinate responses in high-pressure situations.
4. Strengthen Decision-Making Abilities: By working through different scenarios, participants will have developed stronger decision-making skills, allowing them to prioritize actions, mitigate risks, and allocate resources during an incident.
5. Recognize Gaps in Cybersecurity Posture: The exercise will reveal any weaknesses or gaps in the organization's cybersecurity policies, procedures, and tools, providing actionable insights to strengthen the organization's overall security framework.
6. Promote a Culture of Security Awareness: By working through real-world use cases, participants will leave with a heightened awareness of cybersecurity risks and a stronger commitment to maintaining a secure environment in their roles.

This comprehensive exercise will not only sharpen technical skills but also foster a deeper understanding of the importance of a collaborative and proactive cybersecurity culture in protecting the organization.