Tabletop Exercises & Simulations

Cyber Incident Response Testing -
Prepare Your Organization for Effective Remediation

What are Tabletop Exercises & Simulations?

Tabletop Exercises & Simulations should be where and when cyber-attacks become a real-life experience. These are customized cyber-attack simulations on organizations' security programs and IT infrastructures to mimic attacks and breaches specific to industry. These simulations allow organizations to test their incident response plans in a safe environment, determine whether they are effective, and apply specific methods to improve them.

These "real-life" incident simulations enhance response plans from every angle. Security gaps within the current defense plan are closed, creating a resilient program in the event of an incident. Tabletop simulations run through all aspects of response from the moment the threat is discovered to how it is communicated to the media.

How do Tabletop Exercises & Simulations work for me?

1. **Scenario development** - incidents appear real. Scenarios are designed to allow the team to discover gaps and issues during the engagement.
2. **Tabletop exercise** - a discussion with the staff on their roles and responses in hypothetical situations (doesn't require extensive preparation or resources). Tests the team's understanding of their incident response roles.
3. **Simulation exercise ("War-gaming")** - testing incident response processes through a live walk-through. Allows team members to experience events in real time and helps them understand their roles.
4. **Plan development** - develop and document the organization's incident response playbook. Ensures that everyone in the organization is on the same page, knows their role, and will execute processes in the same way during an incident.
5. **Executive briefings** - a high-level compilation of lessons learned from the exercises, including a summary of how participants worked with the organization's incident response plan, communications plan, and escalation procedure.
6. **Report and action plan** - a report with a timeline of events, detailed analysis of participant and stakeholder activities with strategic and tactical recommendations for improving detection, response, containment, and remediation.

WHAT SHOULD YOU EXPECT?

- **Controlled real-life simulations of incidents specific to the industry.**
- **Scenarios include malware attacks, unauthorized access, ransomware attacks, cloud compromise, and more.**
- **Gap analysis of the current incident response and remediation plans from both the technical and business perspective.**
- **Unbiased validation of the success points in current plans.**
- **Organizations receive a tested plan to amplify cyber incident resilience.**
- **Increased confidence and communication outside of IT and security departments.**
- **Closing communication gaps throughout the organization.**
- **Increased security awareness.**
- **Enhanced communication between teams.**
- **Scenarios based on known attacker behavior, tactics, and techniques.**
- **Outlining the organization's threat profile, the operational environment, and specific areas of concern.**

Skilled facilitators guide the exercises, analyze the organization's incident response and management capabilities from all aspects, and ensure that response and recovery plans are well coordinated and communicated. They also keep participants focused on exercise objectives. Typically, several scenarios that could profoundly impact the business are simulated. Internal and external stakeholders, C-level executives, and the company's security team participate.

War-gaming, the cyber role playing game.

- Use the response plan as a road map.
- Simulate full event: from incident discovery to media relations and remediation
- Review gaps in the plan.
- Update the plan based on gaps found.

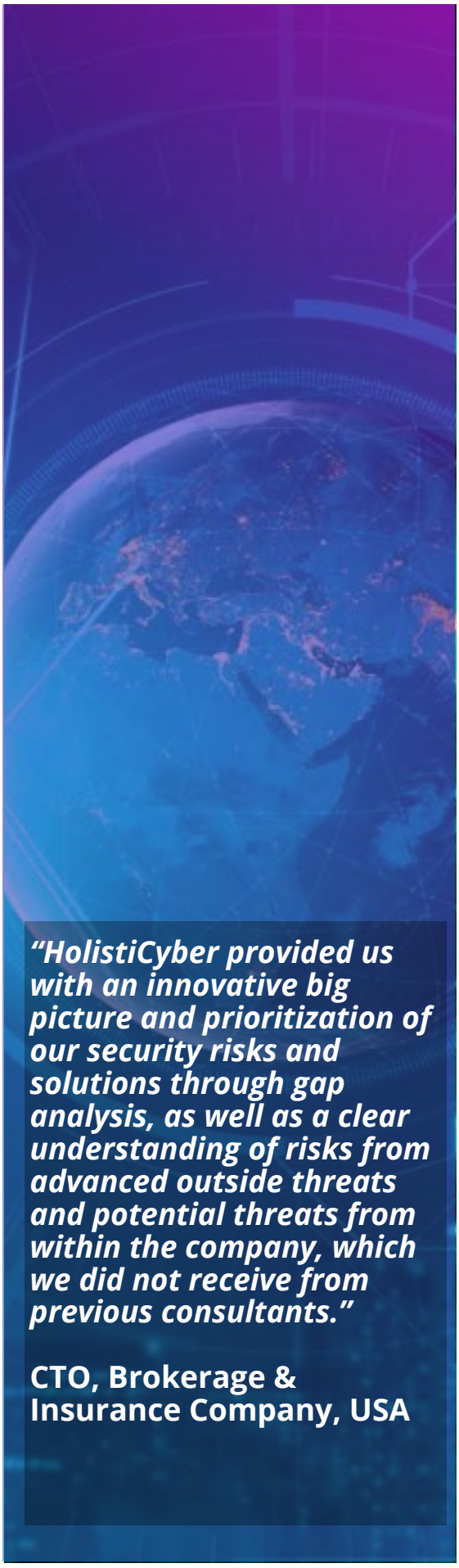
How can enterprises keep up with today's cyber threats? By getting ahead of them.

Often, organizations get blindsided when an incident occurs, even with a proper plan in place. From the responders to the PR professionals handling the story coverage, many moving parts go beyond remediation of the incident itself. A controlled incident environment to rehearse execution is critical to a security strategy. It is too late to discover gaps in the organization's response plan when an incident occurs.

Tabletop exercises and simulation services provide an excellent tool for organizational awareness, staff training, and preparation for security incidents. The services ultimately allow teams to come together and determine whether the response plan is effective and how to improve it before an incident occurs.

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.



"HolistiCyber provided us with an innovative big picture and prioritization of our security risks and solutions through gap analysis, as well as a clear understanding of risks from advanced outside threats and potential threats from within the company, which we did not receive from previous consultants."

CTO, Brokerage & Insurance Company, USA