MAYER·BROWN

MEDIA COVERAGE

10 Tips for Planning, Leading and Learning From a Cybersecurity Tabletop Exercise

8 December 2016

Corporate Counsel

Effective responses to cybersecurity incidents rely in large part upon three key elements: personnel, planning and practice. An organization's incident response team must include capable personnel with the appropriate authority to act, requisite expertise and adequate training. An organization also needs a written plan customized to meet its business, industry and regulatory environment, among other things.

But the right people and a well-written plan are not enough. An organization's incident response team and other key stakeholders must practice responding to incidents. Although practice does not make perfect, it usually enables people to perform better when called upon.

The National Institute of Standards and Technology (NIST) recommends that organizations not only develop incident response plans, but also maintain them in a "state of readiness" and engage in exercises to "validate their content." The potential vehicles for such tests can take many forms, but one of the most common and easy to implement is a "tabletop exercise."

Tabletops take the team members responsible for responding to incidents (along with other key stakeholders), put them in a room and ask them to work through the implementation of their response plan against one or more scenarios. It is an inexpensive, direct and powerful method for revealing the weaknesses in a given incident response framework before an incident actually happens. Tabletops have long been employed to test emergency response and business continuity plans in government and the private sector, and are becoming commonplace in the cybersecurity toolkit. NIST recommends them, and in 2012 the Federal Emergency Management Agency released a "cyber scenario-based exercise" for companies to use in their preparations. And growing numbers of industry groups and individual companies are organizing their own exercises to augment their capacity to detect and respond to incidents.

Here are 10 tips for planning, leading and learning from a tabletop exercise.

1. When to conduct a tabletop: To maintain and practice a plan, businesses should consider conducting a tabletop exercise on at least an annual basis, depending upon the organization's threat profile. However, it is also a good idea for an enterprise to practice its incident response plan after experiencing a significant change in business activities, hardware or personnel. Is there a new key member of the incident response team who must be integrated? Has the organization recently acquired a new business line with a distinct threat profile? Has the IT department recently upgraded hardware or software in ways that require revising the incident response plan? Any of these changes could warrant conducting an exercise.

2. How to initiate: A tabletop is a comparatively simple and inexpensive way to stress-test an enterprise's policies and plans. But it still requires management buy-in and a commitment from participants. Success will depend upon the organizers' ability to get necessary resources and robust participation, Company leadership should both support the exercise and explain its utility and business necessity. For example, for tabletops that require participation of multiple corporate departments, an invitation from a senior executive can help ensure broad participation. Also, conducting this exercise outside of the normal business hours helps ensure the availability of the key participants.

3. What to focus on: A tabletop is a limited exercise; it cannot explore every threat or response process. Rather, a company's exercise should reflect its threat trends, vulnerabilities and assets. This analysis can build upon an enterprise's risk assessment. Whether the organization faces insider threats, nation-state actors or criminal organizations, the tabletop should reflect likely adversaries and likely exploits. For example, while businesses with significant intellectual property might construct an exercise focusing on data theft, an energy company might be more concerned with the integrity of industrial control systems.

4. What to include: The exercise should do more than just focus on an incident response plan line-by-line. No real crisis response will be so tidy. To add realism, tabletop scenarios can test coordination with other key programs, such as business continuity, disaster recovery and/or compliance. Exercises also can incorporate potential interactions with the media, customers or clients, federal or state regulators and law enforcement officials (as appropriate). No incident takes place in a vacuum, and the exercise can reflect this fact by requiring participants to deal with external factors that are thrown into the mix.

5. Whom to include: The participants should include all members of the incident response team and other appropriate stakeholders and parties. Organizers should identify appropriate individuals to facilitate the exercise and manage its execution. External team members, such as outside counsel, crisis communications professionals or forensics examiners, often participate to simulate how the enterprise would respond to a real incident. These external players will have experience participating in or leading tabletops at other organizations, and may have valuable insights to share.

6. How to plan: The value of this exercise will increase exponentially in relation to how much planning goes into it. Organizers should draft a detailed script of events and be prepared to circulate unexpected developments to participants as the story unfolds. This script will have a parallel timeline to help participants appreciate the real-world timing and delays that can impede a response. It is also important that at least one nonparticipant observe the exercise and take notes.

7. What type of scenarios: Tabletop scenarios often have the potential to expose coordination breakdown or highlight areas for improvement. Scenarios also frequently simulate events that would demand unexpected combinations of response activities, disrupt normal business or contingency processes, and/or challenge participants to adapt the procedures they have already developed to novel or unfamiliar problems. For example, one tabletop conducted by the Financial Services Information Sharing and Analysis Center began with maintenance locating a non-standard issue smoke detector plugged into a network cable and concluded with a crippling DDOS attack.

8. How to facilitate: Effective planning can help ensure that participants engage meaningfully in the scenario and fulfill their roles as if the event were real. Ground rules for how the exercise will work should be communicated clearly to all participants before it begins. However, because the purpose of the exercise is to train the participants, the facilitators should be prepared to step in if participants appear flustered, embarrassed or unsure of what to do next. It is important for facilitators to communicate that the exercise is not a test seeking to grade participants on whether they have the right answers. Rather, it is an opportunity to improve their capacity to respond to incidents, and for the company to fine-tune its incident response plan and other policies.

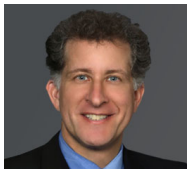
9. How to conclude: The primary value of tabletop exercises comes from the lessons distilled from them. Every tabletop should conclude with an "after action review," discussing what worked well and what aspects of the incident response plan or other policies need improvement. A tabletop could also reveal that while the policies are adequate, employee training is lacking or better internal coordination is required. Organizers can solicit input from participants on both the substance of the policies and the character of the exercise. Did the scenarios, information flow, timing and challenges seem realistic to the participants?

10. What to do afterward: Lessons learned from tabletop exercises must then be incorporated into relevant plans and policies. After exercise organizers gather and analyze information from participants, an individual with the requisite authority should ensure that the company's incident response policy and other appropriate policies and practices are modified to reflect the lessons learned. For example, if the tabletop reveals that the incident response is vulnerable to attacks that compromise primary communications systems, then the organization can revise its plan to include provisions for secure backup communications.

An effective tabletop exercise can help a company improve the effectiveness of its response to an actual cybersecurity incident, which will mitigate the potential legal and reputational harm that arises from one. And there's nothing bad about that.

Related People

Marcus A. Christian
Partner
T +1 202 263 3731
mchristian@mayerbrown.com



Jeffrey P. Taft
Partner
T +1 202 263 3293
jtaft@mayerbrown.com

Joshua M. Silverstein
Associate
T +1 202 263 3208
jsilverstein@mayerbrown.com