MAYER·BROWN

Cybersecurity Tabletop Exercises

Cybersecurity Tabletop Exercises

As large-scale cybersecurity incidents dominate headlines, we regularly work with clients to practice and test their policies through realistic, tabletop scenarios. Tabletops gather the team members responsible for conducting an incident response, present them with a fictional scenario and ask them to analyze how they would implement their company policies and procedures—incident response plans, playbooks, and related documents—to address that situation. These exercises can reveal what works and, more importantly, what does not in the way that a company intends to respond to an incident.

EXPERIENCE

We have led or participated in tabletops for numerous clients in a variety of sectors, including the automotive industry. These exercises have addressed a wide range of scenarios, including nation-state intellectual property theft, point-of-sale incidents, connected device compromise, vehicle cybersecurity incidents, distributed denial of service attacks, destructive malware or ransomware incidents, and vendor data breaches that compromise customer personal information.

MULTI-PARTY EXERCISES

We regularly work with in-house legal teams and cybersecurity experts to tailor exercises to risks identified by an organization's threat profile and incorporate details unique to the organization's operations and assets. We also have capabilities and experience engaging with other external partners to conduct highly realistic exercises. For example, at a recent event, members of our Cybersecurity & Data Privacy team, along with representatives from CrowdStrike and Brunswick Group, conducted a cybersecurity tabletop exercise with senior representatives from more than 40 companies across a variety of industries.

Project Phasing. Our support for clients in conducting tabletop exercises can be phased according to client needs and budget. An illustrative example of such a phased approach is provided below:

Phase 1: Tailoring and Preparatory Work: This phase would entail a limited and focused investigation of a company or organization's cybersecurity program, with a clear emphasis on incident response plans, policies, procedures and documents. This investigation and subsequent analysis would facilitate tailoring the tabletop exercise to a company or organization's existing approach to cybersecurity incidents.

Phase 2: Engagement with Vendors: In a real-world cybersecurity incident, a company or organization is likely to leverage the support and expertise of external partners. Including these partners in a tabletop exercise can substantially increase the verisimilitude of the experience. We can support a company or organization in identifying and selecting vendors or engage pre-selected or preferred vendors that a company or organization has already identified.

Phase 3: Creating a Tailored Tabletop Exercise: In this phase, Mayer Brown would independently, or in concert with participating vendors, develop the content and materials for the tabletop exercise. We

have experience developing a range of exercises from paper-only discussions to sophisticated simulations that leverage the expertise of production companies and other vendors to create compelling audiovisual presentations or "injects" to augment the realism of the exercise.

Phase 4: Participating in a Tabletop Exercise: We can leverage substantial experience both leading and participating in tabletop exercises to enhance the value of a company or organization's investment in this simulation.

Phase 5: Developing an After-Action Report: To benefit fully from conducting an advanced tabletop exercise, it is valuable to employ a formal process to capture key conclusions, recommendations or items for further investigation. This phase could entail the development of a privileged whitepaper or senior leadership briefing materials.