Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

Five Questions General Counsels Should Ask about Cybersecurity Tabletop Exercises

As large-scale cybersecurity incidents dominate headlines, companies should consider how they can prepare to manage and respond to such potentially damaging events. With cybersecurity maturity growing across economic sectors, the importance of establishing written policies and procedures—and implementing them—has become axiomatic. What may be less obvious is the vital importance of *practicing* those same policies and procedures. Just as companies subject their digital defenses to penetration testing and red teaming, so too should they test the policies and personnel responsible for cyber incident response against realistic incident scenarios in a trusted environment. One vehicle for such testing is a tabletop exercise. 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 to address that situation. These exercises can reveal what works and—more importantly—what does not in the way a company intends to respond to an incident.

Lawyers from our Cybersecurity & Data Privacy practice lead tabletop exercises with clients across economic sectors. At a recent event, the 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. Below we identify some of the key questions raised by this exercise.

Why Would You Conduct a Tabletop Exercise?

Tabletop exercises are a valuable tool to improve cybersecurity and incident response readiness. At the same time, they can validate portions of existing plans and highlight areas for improvement or revision. Moreover, they are generally inexpensive and can yield significant benefits with minimal investment. The US government has encouraged companies to conduct tabletop exercises. For example, the National Institute of Standards and Technology ("NIST") has recommended that organizations not only draft and implement incident response plans but also use exercises to "validate their content." Federal regulators increasingly expect companies to not only possess plans but also train and prepare to implement them—potentially through tabletop exercises. Finally, as companies work to mitigate cybersecurity risks and consider the benefits of purchasing cyber insurance, conducting tabletop exercises that validate and/or improve existing practices can have a material impact on the cost of insurance premiums.

How Should You Structure a Tabletop Exercise?

At a basic level, an exercise should present participants with a scenario that develops over time. That development occurs through the use of "injects" that add new facts and complications. The more planning that goes into developing the

scenario and injects, the more valuable the exercise will be. One key way to add value to this experience is to ensure that the content of the exercise is keyed to the specific risks facing an organization. What attack vectors would a malicious actor be most likely to use? What assets would an attacker seek to access? The answers to these and similar questions should inform the substantive content of the exercise. Additionally, while it is obviously important to test the basic functions of the incident response team, it is also useful to see how that team will interact with the organization's other business and support units, such as human resources, business continuity, and disaster recovery. Finally, it is always valuable to task at least one non-participant with observing the exercise and taking notes to be used for after-action analysis.

Why Would External Partners Participate in a Tabletop Exercise?

In real cybersecurity incident responses, companies commonly involve external partners. A cybersecurity forensics firm can provide the technical expertise to conduct extensive analysis of logs and network systems to identify vectors of attack and determine the degree of compromise. Many of these firms have wide-ranging experience and can identify industry trends that might not be apparent to a single entity. Likewise, a crisis communications firm specializes in the high-pressure, high-stakes internal and external communications challenges that a business's communications unit seldom faces. Finally, corporations often turn to outside counsel during incident response for legal advice informed by experience with numerous cybersecurity incidents and follow-on litigations or regulatory investigations. Tabletop exercises can bring together these key players and a company's internal response team to work through a realistic scenario. Among other things, this helps external team members understand the practical aspects of a company's formal policies and the dynamics of corporate culture and individual personalities. Moreover, external participants can leverage their experiences from other incidents and exercises to a company's benefit.

What Role Should In-House Counsel Play in an Incident Response?

There is no single right answer to this question. The role of in-house counsel in an incident response will depend on the experience of counsel, the role they play within the organization, the skills and expertise of other members of the incident response team, and the nature of the incident. In some cases, in-house counsel will serve as the "quarterback" of the response, intimately working with forensic investigators and crisis communications personnel to address every facet of an incident response. In other cases, their role might be more limited or delegated to outside counsel with substantial experience in responding to cybersecurity incidents. A tabletop exercise can help illustrate what role in-house counsel should play in a particular organization's incident response process and provide a trusted environment in which to practice that role. While every organization is different, it is important to consider that the degree of counsel—both in-house and external—involvement in directing the incident response process will impact the degree of potential legal privilege protection over sensitive documents and materials related to the response. When legal counsel does not direct the investigation, it can be challenging to protect documents related to the investigation from discovery in civil or regulatory proceedings.

When Can an Organization Safely Stop Conducting Tabletop Exercises?

The simple answer is never. As organizations change, the need to practice responding to the panoply of possible cybersecurity incidents remains constant. New employees need to be integrated into response teams and educated on

their roles. The impact of new technology—such as cloud storage or internet-connected devices—needs to be assessed. And new business acquisitions need to be factored into how the organization as a whole will confront a cybersecurity incident. Tabletop exercises allow companies to see how new people, processes and technology impact overall incident response readiness. They are part of an iterative process in which each exercise reveals new challenges or gaps that foster revised plans, which must in turn be tested. These efforts constitute a vital investment in an organization's security that can pay dividends when a response team functions effectively to contain a real incident efficiently. While it is true that organizations are never "done" with holding exercises, many observers ask how frequently organizations *should* conduct exercises. The answer will ultimately depend on the risk profile of the organization. The frequency of tabletop exercises should be risk-based and keyed to major changes in people, processes and technology, but, as a rule-of-thumb, executives should consider conducting an exercise at least annually.

For more information about the topics raised in this Q&A, please contact any of the following lawyers.

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

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