ALM | LAW.COM

New York Law Journal

This Is Not a Drill: Table-Top Exercises Aren't Just a Good Idea, They're Mandatory for Many Organizations

By **Daniel J. Altieri and F. Paul Greene**
March 1, 2023

In today's age, companies are always looking for the next, best, high-tech way to stay ahead of cyber criminals. Most of the time, this means increased budgets for improvements, such as artificially intelligent security tools, 24/7 systems monitoring and hardened perimeters. This isn't a bad thing, of course, given the omnipresent cyber risk faced by organizations of all types and sizes, and the inevitability of security incidents.

However, with all that focus—and spending—on artificial intelligence, it's sometimes easy to forget about the importance of developing *actual* intelligence—of humans, that is. Conducting regular table-top drills to test and expand the knowledge of incident responders and the strength of incident response plans doesn't cost much, but it does wonders maximizing incident response efficiencies and minimizing confusion in the wake of an incident. And if those reasons were not convincing enough to conduct table-top drills, they also help ensure that an organization remains in compliance with potentially applicable law.

A table-top drill involves bringing the entire incident response team together into one room, virtually or otherwise, and running through mock incident scenarios to test response efforts in relation to cyber incidents of all types, including ransomware,

Daniel J. Altieri, left, and F. Paul Greene, right, of Harter Secrest & Emery. Courtesy photos

insider threats and business email compromises. These exercises aid in an organization's effort to identify risks from technical, legal and operational perspectives, while encouraging open and frank discussions regarding real-world response strategies in a low-stress, collaborative environment.

A key component of a table-top exercise is ensuring that all members of an organization's incident response team know their respective roles and how they will fit into response efforts in the event of an incident. With the direction and oversight of legal counsel, these exercises can and should also be protected under the attorney-client privilege, shielding any discussions or resultant work product from potential disclosure to third-parties.

Unfortunately, however, notwithstanding the proven and substantial benefits of table-top drills, many organizations are still not performing them on a regular basis. Other organizations are running perfunctory or purely technical drills as a "check the box" activity, but forgetting to involve key organizational decision makers, like senior management. Often, the most important aspects of incident response are non-technical and the biggest mistakes an organization can make derive from management's lack of familiarity with the incident response process.

Perhaps the main hurdle in conducting a table-top drill and securing the right people at the table is scheduling. Indeed, carving out a half-day or more calendar block for the whole incident response team, consisting of an organization's key stakeholders and top-level executives, is no easy task. But when considering that a failure to hold regular table-tops could lead to a violation of law, fines, and other penalties, scheduling challenges should seem less insurmountable.

To be clear, even with the continued proliferation of data protection laws throughout the country, adding to the already complex patchwork of overlapping schemes, without any overarching, generally applicable statute, not all of these laws specifically mention table-tops. That is not to say that any interested regulator would agree that companies do not have to conduct them. For example, New York's SHIELD Act, N.Y. G.B.L. § 899-bb, which became effective as of March 2020: while the word "table-top" (or "incident response plan," for that matter) is not found anywhere in the Act, organizations subject to the Act, which include every employer in New York, must employ reasonable "administrative safeguards," including by "train[ing] and manag[ing] employees in the security program practices and procedures."

Certainly, table-top drills qualify as training in this regard and, given that businesses in violation of the Act are "deemed to have violated" New York's prohibitions against unfair and deceptive conduct in trade, N.Y. Gen. Bus. Law § 349, it's far safer to simply conduct table-top exercises than it is to rationalize that they are somehow not expressly required.

Indeed, in this regard, it is important to consider that regulatory scrutiny after an incident is often 20/20 and negative: if a problem occurs in relation to incident response, one of the first questions from a regulatory authority will concern the organization's incident response efforts and preparations for them.

Other potentially applicable statutes are clearer. The Federal Trade Commission's Safeguards Rule, 16 C.F.R. Part 314, with new amendments becoming effective on June 9, 2023, explicitly requires financial institutions to "establish a written response plan designed to promptly respond to, and recover from" security incidents. Of course, as a practical matter, a "written response plan" is of no value to an organization, unless it is tested.

And recently proposed amendments to the New York State Department of Financial Services cybersecurity rules, 23 N.Y.C.R.R. Part 500, go even further, not only requiring companies subject to the regulations to adopt incident response plans, but also requiring them to "provide relevant training to all employees responsible for implementing the plans regarding their roles and responsibilities" and, at least annually, test their incident response plans "with all staff critical to the response, including senior officers and the highest-ranking executive at the covered entity."

If adopted, this express requirement will likely usher in a new wave of similar changes to existing laws: mandatory annual table-top drills. Such an annual requirement already exists under the Payment Card Industry Data Security Standard, which applies to organizations that accept or process payment cards. But given the influential

nature of Part 500—which has been emulated by several states and has become a common benchmark for security compliance—this new requirement will likely be adopted elsewhere too.

Indeed, further foreshadowing that likelihood is a recent Assurance of Voluntary Compliance entered into in November 2022 between Experian and dozens of State Attorneys General (including New York's) arising from a massive data breach suffered by Experian in 2015. In exchange for releases provided by the Attorneys General, the Assurance, among other things, expressly requires Experian to "conduct, at a minimum, bi-annual incident response plan exercises ("table-top" exercises) to test the sufficiency of [its] incident response plan and assess its preparedness to respond to a Security Event." (parenthetical in original).

As the regulatory backdrop evolves and legislatures continue to devote more focus to incident response planning, some organizations are surprised by what they perceive as new and more stringent requirements. As indicated above, though, such planning has always been an important piece of an organization's compliance efforts.

Regular response plan testing is a critical, but yet often overlooked, component of an organization's incident preparation efforts. Table-top drills allow incident response team members to develop muscle-memory in the event of a real incident, which streamlines and often shortens the duration of response activity.

They also, as discussed above, help demonstrate legal compliance against constantly evolving mandates that generally require an organization to assess risks pertaining to cyber security and, increasingly, more specifically, require team members to receive training on the response plan, upon which they will rely when an incident occurs.

Organizations should therefore devote necessary efforts and resources to conducting table-top exercises on a regular basis or otherwise redouble their commitments in the event of already mature testing programs.

But with repetition comes the danger of complacency: although regular testing is key, the challenge remains to keep such testing relevant and engaging. Table-top exercises should not be viewed as a mere compliance requirement. Rather, such drills should be viewed as a unique opportunity to build team spirit and appropriately assess and manage risk. A drill may reveal holes in a plan, areas for potential improvement, or otherwise identify processes that may not be workable for a specific organization.

Often, for example, it is only in a drill scenario that an organization identifies the uncatchable legacy server, no longer needed but now end-of-life from a software perspective. And after an incident or drill, it is important to ensure that the incident response plan is revised to address such gaps, to ensure that it remains tailored to the changing needs and risks of the organization. Follow-up one-on-one sessions should be conducted with each member of the incident response team to ensure familiarity and comfort with roles, and to determine whether any adjustments in role allocation need to occur.

In the end, a table-top drill brings value to the organization well beyond abatement of compliance risk. Thus, whether or not an organization is required to conduct a drill, few organizations can reasonably justify forgoing one.

Daniel J. Altieri *and* F. Paul Greene *are partners in the Privacy and Data Security practice at Harter Secrest & Emery, LLP. They can be reached at fgreene@hselaw.com and daltieri@hselaw.com.*