HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

November 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

The Evolution of Healthcare Law and Compliance

an interview with Sara Kay Wheeler
2015–2016 SCCE/HCCA Board President
Partner, King & Spalding

See page 16

by Benjamin Winkler, CHC, MBA, JD

Gamifying breach response tabletop exercises

» Tabletop exercises are essential to testing breach response plans.
» Exercises are more interesting and effective if they "gamify" scenarios.
» Create a simulated situation with a particular time and conditions.
» Run the exercise in turns, representing a couple hours each.
» Add simulated complications, so you're not testing a best-case scenario.

Benjamin Winkler *(bwinkler@covermymeds.com) is Manager of Regulatory Compliance at CoverMyMeds in Columbus, OH.*

Every organization should have a plan in place for responding to a data breach. It is also essential to conduct tabletop exercises to test your breach response plan, to make sure that all the key players are familiar with their roles *before* the plan is suddenly put to the test. However, if your organization's exercise amounts to everyone following along while you read through a breach response flowchart together, it can be hard to muster much enthusiasm among participants for being pulled away from their day jobs.


Winkler

"Gamification"—adding gaming-like elements to improve processes—offers a way to present a more engaging and effective tabletop exercise. The organizer or moderator can design and run through a simulation with enough realistic elements and complexities that the participants get a sense of what it would actually be like for breach events to unfold. This can better reveal critical gaps in the response plan, permit reality checking for how long certain response measures would really take, and demonstrate whether the plan actually works if it isn't a best-case scenario. First, work out a complete situation. (Example: A breach is discovered during the night shift by a nurse; 600 patient records were accidentally faxed last week to an unknown number. The employee responsible is currently on vacation. The fax number turns out to be an unrelated business out of state. The recipients didn't know what to do and called their lawyers.) Next, let participants play it out to see how the breach response plan would handle it.

Developing an engaging scenario

The following are some practical ways to develop a tabletop exercise into an engaging scenario.

Set the stage

The first thing the moderator should do is to make sure that all the participants understand that the exercise will simulate a specific scenario. Describe the setting—it makes for a richer experience if the participants understand that the situation is happening on June 29, 2017, or during the busy season, or during the university's Homecoming week. Describe where everybody "is." Everyone could simply "be" at work during the simulated incident, but what if the CEO is at

a meeting in Singapore and hard to reach for two days, and the technical infrastructure lead is at a vendor conference for the week?

Keep a clock

The moderator should have the exercise proceed in defined time phases. The simulation starts at Day 1, Hour 1 (or 9:00 AM on June 29, or whatever works best). Each phase should represent the same time interval, such as an hour or half a day. The moderator announces when a time phase has "elapsed," either on a fixed time schedule, such as five minutes, or when all the participants have determined what they would do in the phase. Consider adding in some events that unfold or facts that are discovered, which the moderator can announce at the appropriate time (e.g., the phones go down, the receptionist reports that a newspaper reporter has arrived and is asking questions about the breach).

Control the release of information

Keeping track of time allows the moderator to have events unfold at appropriate times. If a forensic examination is requested at Hour 3, and it would take two hours, then the moderator provides the "results" at Hour 5. If the CEO is giving a keynote speech from Hour 6 to Hour 8, then nobody can inform him of anything or request anything during those phases. If the newspaper reporter arrives at Hour 7, then it can be revealed at Hour 8 that an employee accidentally leaked news of the situation to a friend outside the company.

The moderator should give out information to all participants if they realistically would receive it, such as an announcement that the phones are working again. Otherwise, information should be given privately on a note card to one person. Don't announce that "the chief technology officer (CTO) finds out that the database has been corrupted by someone outside the company." Give the CTO this information on a card, and then she can follow along and advise other individuals according to the breach response plan — or discover, usefully, that the plan doesn't really cover what to do next.

The plot thickens

As noted above, a tabletop exercise can be a lot more useful if it doesn't run through the smoothest, best-case scenario or doesn't simulate the situation the planners had in mind. Here are some ideas to add complexity.

An inside job

No one wishes to encounter such a situation, but dishonest or malicious employees are always a possibility. Reveal information to the participants partway through that the breach took place as the result of a deliberate leak by an employee. Only hypothetical employees should be used, obviously, but there are many possibilities.

Scenarios:

- A billing supervisor emailing out records in a misguided attempt to "prove to management that security is flawed";
- A developer with an addiction problem selling a database password; or
- The CTO could get this card: "You get a text message from one of the database administrators. He found the missing logs from the breach, but also found that it was Bob, his manager, who deliberately deleted them. He thinks the audit trail shows Bob downloaded the records and then covered it up. Bob is here, at work, right now. The database administrator wants to know what to do." What *would* the CTO do?

Adverse weather

If appropriate for your area, consider how events would unfold if a hurricane threatened to make landfall during the scenario's time period. At different time intervals, the moderator can give updates about whether or not

evacuations or other factors come into play. How would assessing the extent of a breach be affected if the company suddenly had to switch to its backup data center due to widespread power and network outages? For other states, set the exercise during a blizzard. The breach response plan may rely at one point on a team from Marketing to promptly send out customer information, but are they essential personnel who would even be on site on Day 2?

Complications

Have the scenario be more complicated than it first appears. For example, set the incident up, and present information initially as if it had been an electronic intrusion to steal records. Then, at Hour 2, slip the Help Desk supervisor a card advising him that someone is on the phone claiming it is a ransomware attack, and that the caller has instructions for how the company can pay the ransom.

Alternately, reveal part way through that the breach didn't actually take place—the briefcase was reported lost due to a misunderstanding, or the hacked files were personnel records, not patient files. However, customers and the media all think a breach occurred. Now what?

Conclusion

Designing and running through a gamified breach response simulation will take more work than a simple tabletop exercise where everybody affirms what the response plan requires and traces the flowchart. However, a scenario where the local newspaper publishes reports of an athlete's confidential lab results, and your organization is scrambling to find out what happened and what to do next, will enjoy better participant interest. It will also raise more of the right kind of questions: Does this breach response plan work only on paper, or would it work in real life? Does everyone know what to do? Is it missing anything? What if…?