Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Run A Data Breach Fire Drill

By **Melissa Maleske**

Law360, Chicago (January 13, 2016, 4:54 PM ET) -- When a data breach hits a company, it delivers a healthy dose of stress, panic and urgency — and it's just about the worst environment for an incident response team to put its procedures into action for the first time. But GCs can help their organizations conduct a cybersecurity simulation to ensure that when the real one arrives, everyone's ready.

"I think in the very near future, this is going to be absolutely expected of all companies by regulators," says Steptoe & Johnson LLP partner Michael Vatis, the founding director of the Federal Bureau of Investigation's National Infrastructure Protection Center and former associate deputy attorney general and deputy director of the U.S. Department of Justice's Executive Office for National Security. "Because it's one thing to have a paper plan sitting in a binder on a shelf that nobody's ever looked at since it's been written, and then a big incident happens and no one knows how to use the plan or they realize this is not helpful at all."

From the moment a breach is revealed, an incident response team needs to be able to get into formation and respond to a crisis that will yield new demands and challenges by the minute. If the team members have practiced and refined their response, they're much more likely to minimize damage to the company, its systems and its clients or customers whose information might have been stolen or compromised.

Then, in investigations and litigation that are common after a significant breach, regular exercises will show that the company was as prepared as they could have been.

"In defending a breached organization, I absolutely would prefer to defend an organization that has done an annual incident response exercise to defending one that has not," says Lori Nugent, a shareholder at Greenberg Traurig LLP. "One of the things we look for when a breach happens is what evidence we have that a company has done appropriate and prudent things to prepare for a breach in addition to working to avoid a breach."

A natural part of preparedness is testing out your plan and making sure it's right for the company.

Prepare to Practice

Just as you wouldn't run a fire drill without first establishing where the exits are located and who will lead participants to them, you shouldn't host a breach response exercise without first appointing a team and educating them about the breach response plan’s policies and procedures.

"It's much more helpful if people come in prepared," Vatis says. "Then you're really testing your incident response plan. If they don't know what their response plan is, you're not really testing the plan at all, you're testing those individuals who may come to the table with no understanding of what their plan is."

If that's the case, Vatis recommends running another exercise very soon after the first one so the team can apply the basics they learned on their feet during the first exercise.

As for who should comprise the incident response team, at a minimum it should include all the senior managers in any department that might be implicated in a breach. The team should include the chief executive officer, chief operations officer, chief financial officer, compliance head, chief information officer, chief information security officer, physical security head, human resources head and the communications director. And the legal team will of course play a integral role in guiding the team and its response, even if many of those calls are ultimately made by the CEO.

"Legal decisions are going to have a very prominent place in incident response," Vatis says. "A lot of times, companies go in thinking this will largely be a technical issue for the CIO or CISO and if they just throw resources at it, they can fix it through technical measures. They don't realize that the GC is going to run the show to a very large extent."

Involve Outside Counsel

There are a few good reasons to get outside counsel involved. First, the general counsel, compliance officer and in-house lawyers should be active and key participants in the simulation and need such a training exercise just as much as others in the company. Outside counsel can design and run the simulation so the legal department team can be fully immersed in the exercise and able to test themselves on handling unexpected scenarios.

Outside counsel can also draw on their likely extensive experience handling breach responses for clients to customize the exercise for the company based on what it's most likely to see and the challenges it is likely to face.

But perhaps most importantly, outside counsel can help when it comes to privilege. As Devore & DeMarco LLP partner Joseph DeMarco points out, in-house counsel do not enjoy the same cloak of privilege outside the United States.

"For the maximum global protection, you want outside counsel to be running the tabletop because, after all, as these hypotheticals are discussed and people are taking notes, talking about it or even recording it, you don't want to have discovery pulling up your prior tabletop in an actual event two years down the road," says DeMarco, a former assistant U.S. attorney for the Southern District of New York who founded and headed the Computer Hacking and Intellectual Property Program and a former visiting trial attorney at the DOJ's Computer Crimes and Intellectual Property Section.

"It's not airtight, nothing's hermetically sealed, but you maximize the degree of protection and confidentiality by having outside counsel run the exercise," he says.

Test Lines of Communication

Likely the biggest lessons you'll learn and the biggest challenges you'll face during a breach simulation

will come back to communication and whether the people on the incident response plan are effectively gathering and imparting information both among themselves and with other key stakeholders, such as the board.

"[After the exercise,] a lot of the assessment will involve human interaction," says Claudia Callaway, a partner at Katten Muchin Rosenman LLP. "How seriously did people take this? Where did communication break down? Where did misunderstandings arise?"

A good simulation will turn up the heat for participants and force them into communication in extremis. And if someone crumbles under pressure rather than taking a leadership role, it might reveal he or she is not right for team.

"It's when you stoke the fires or when there's a history between people [that communications can break down]," Callaway says. "Sometimes, you have to determine: Is this the right person to be in this role? Is this person responsive and good in a crisis, even a manufactured crisis? A tabletop exercise is designed to look at system quality and to facilitate the best in human communication."

The simulation is also a good chance for team members to get acquainted with one another so that they have established some level of comfort and rapport outside the pressure cooker of a real-life breach response. Nugent says teams should continue meeting outside simulations — even a regularly scheduled pizza lunch can help develop an esprit de corps that can really benefit members as they work through difficult issues.

"A lot of times when we do the exercise, this is the first time the team has physically met in the same place ever. Particularly when an incident response team is broad-based, it can be the first time that the organization gets its arms around the scope of the enterprise risk that cybersecurity is and the management that's required," she says.

Face Hard Questions

During a breach, you'll be forced to make tough calls under high stress. The right simulation will force you to discuss those situations ahead of time. Most companies' IT departments are well situated to handle business continuity, disaster recovery and technical solutions, DeMarco says.

"What they really should be thinking about is not how technically to handle a virus, attack or theft of customer [personally identifiable information], but what are the legal and managerial decisions that the CEO, the COO and the board will need to make in that kind of crisis situation," he says.

For example, it may be well-known in which states the company has a legal obligation to notify customers that their personal information has been compromised, but does the company want to limit its notifications to people in those states or notify everyone?

And say law enforcement, aware of the breach, requests that the company not reveal the breach to anyone for two weeks during its initial investigation. Your cyberinsurance policy, on the other hand, requires that you notify your insurers within 10 days. Should you comply with the law enforcement request and risk millions in coverage or nail down the coverage and potentially harm the investigation?

Those are the kinds of managerial and legal decisions that the GC will inform but that the CEO, COO and board will have to decide for the company, and those are the kind of critically important questions

DeMarco says the incident response team should work through before a real breach hits.

Practice Documentation

Nugent says that throughout a simulation, a big part of what she does is ensure the incident response team understands that aspects of what they're doing will likely turn out to be exhibits in regulatory investigations and highly sought after in class action litigation. For that reason, they need to thoughtfully document what's going on and the actions the company takes as the situation unfolds, keeping in mind that any documents created — including internal emails — will either help out the company or the plaintiffs.

"It's not just the pressure of responding to a crisis that's critical to an organization," Nugent says. "It's recognizing that the manner in which they respond will be highly scrutinized and the documentation will be the centerpiece of litigation if there's a significant breach that draws a class action."

Team members should also be able to serve as strong witnesses in post-breach investigations and litigation.

"Being a member of the breach response team is not for the weak of heart," Nugent says.

Rinse and Repeat

Ideally as soon as the exercise has concluded, the team should sit down to discuss how it went: Where were they strong and, more importantly, where did they falter? Outside counsel can put together an incident report based on those discussions, their observations and additional written observations from team members.

Based on those takeaways, new policies and procedures can be developed and incorporated into the response plan, while aspects of the former plan that didn't work can be phased out.

Depending on how well the first simulation went and how much the plan has evolved, you may want to run additional simulations right away, although one annual exercise is typical for many companies.

And breach team members should be made aware that a failure in a simulation is a good thing that everyone can learn from, not a condemnation of their abilities.

"It's in these tabletop exercises that you really want the points of failure to be exposed and to be remedied," Callaway says. "The whole point of this is to expose the weak spots so you can ameliorate them."

--Editing by Katherine Rautenberg and Philip Shea.