ALSTON & BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

WWW.ALSTONPRIVACY.COM

DECEMBER 3, 2015

Effective Cybersecurity: You Have a Breach Response Plan… Now How Do You Test It?

By Kim Peretti and Lou Dennig

Companies in today's data-driven, interconnected business environment are surrounded by potential data breaches. Be it an intrusion from a hacker, a vendor breach or an employee inadvertently sending sensitive information to the wrong business partner, incidents come in a wide range of shapes and sizes. Most companies now have reviewed their incident response policies and procedures to ensure they have some sort of plan in place to guide the company in responding to such events; but that is not enough. It is critical for companies to test their plans so key personnel truly understand the roles they will play and the decisions they will have to make during an actual breach *before* the breach occurs. Indeed, without such testing, a company has little way to gauge whether the plan will be effective for the company in a real live incident.

Before testing begins, companies need to have a strong incident management process in place. One approach to such a process is a three-tiered structure in which companies have a technical response plan to handle the IT and evidentiary aspects of investigating security incidents (and incidents that only require a technical response), a business/legal response plan to address non-crisis security incidents that require legal involvement (often for "privacy" incidents that require notifications to individuals because of potential compromise of their personal information) and a cyber crisis management plan that sits above these plans and brings together an executive-level team to handle incidents that could have a severe impact on the organization from a legal, financial or reputational perspective.

The technical plan and business/legal response plan can often run parallel to one another, with the technical plan addressing how to identify, contain and remediate a security incident from an IT perspective, and the business/legal plan addressing wider organizational response efforts. The business/legal plan should outline key areas of focus, such as how to maximize privilege protections during an investigation and analyze whether legal or contractual reporting or notification obligations have been triggered. For non-crisis incidents, privacy managers and counsel often play a key role in leading response efforts (with assistance from internal and/or external legal counsel). Importantly, the business/legal response plan should include a clearly defined escalation mechanism to trigger the crisis plan for those incidents that prove to be more severe than initially understood.

Finally, with today's threat environment, all types of companies should consider a separate overarching plan to address the security incidents that quickly evolve into an "all-out" crisis for the company, such as those types of incidents faced by Anthem and an entertainment company that experienced a state-sponsored, destructive attack in 2014, and require significant board and executive management involvement. The use of multiple plans can help streamline a coordinated response effort, but it is crucial that incident responders understand how the plans work together rather than merely focusing on each separate plan in a silo.

Having appropriate plans for your business is important, but plans alone are not enough and no plan is perfect. Plans must be tested. Accordingly, companies must break free from planning paralysis, continuously tweaking and adding additional playbooks into the plan itself, often at the expense of testing. One important aspect of a cyber-resilient organization—one that strives to withstand and mitigate the damage from cyber attacks in the face of ongoing threats—is the efficient response to and recovery from security incidents. Such resilience requires devoting resources not just to creating plans, but testing them. A recent study[1] showed that while a strong majority of companies have some form of response plan in place, 37 percent have *never* updated or reviewed their plan, and nearly 70 percent of companies do not feel that their organization is actually prepared to handle an incident response. Fortunately, according to the same study, corporate security professionals know how to make their plans more effective: testing. A full 77 percent of respondents stated that practicing response efforts would improve their plans' effectiveness.

Just as there is no perfect plan, there is no one size fits all testing technique. Nor is there a single moniker for testing, as various entities engage in "scenario planning," "threat simulations," "cyber tabletop exercises" or "cyber war gaming" to name a few. Plan testing is largely an art, not an absolute science, and no matter what you call it, here are five things you need to know about testing your incident response plans:

1. **Start small, work to big.** If most of your core response team members haven't yet read your company's response plans, don't start with a tabletop that tests the plan. Instead, start with a training exercise that familiarizes core members with the newly identified response processes and educates your response teams on their roles and responsibilities and what issues they will have to address during an incident. Follow up that training with a simulated incident response on a relatively simple scenario of limited duration that eases them into the exercise process. No need in the first tabletop to pull the CEO out of a meeting to simulate a true emergency response, though you should plan to work your way to a "near live fire" simulation.

2. **Understand what you are trying to test.** Data breach response requires cross-functional teamwork during what feels like (and sometimes is) a crisis for the company. By stress testing how the unique personalities of your organization interact during an incident, you can take away key insights to make your plan more efficient. For example, while the business/legal response plan may identify the privacy counsel as the response leader, testing may reveal that your chief information security officer (CISO) tends to take charge and may be better suited for that role. Another core purpose of plan testing is identifying gaps in the various plans—testing provides a ready-made forum for organizations to fine-tune their plans and plug identified holes, such as points of escalation and plan triggers. It is important that plans are tested both individually and in tandem so responders can better understand how the plans interact with each other. Testing can also reveal key information unrelated to the plan itself, such as identifying the level of importance business leaders attach to cyber incidents and whether that level of engagement may lead to a response that is insufficiently staffed for the potential risk.

[1] "Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness," Ponemon Institute, September 2014, *available at*: http://www.ponemon.org/blog/is-your-company-ready-for-a-big-data-breach-the-second-annual-study-on-data-breach-preparedness.

3. **Choose the facilitator/moderator carefully.** Have the folks who live in the breach response trenches lead the training exercises and bring their real-world experiences to the table. Seasoned responders can help guide the discussion into a constructive dialogue and, importantly, prevent the group from going down rabbit holes and discussing issues that are unlikely to come up. Experienced moderators know the pitfalls companies have actually fallen into and can help your organization learn to identify and avoid them. Forensic investigators, crisis managers and outside counsel have a sophisticated understanding of the life cycle of an incident and the typical patterns of response behaviors and thus make for effective facilitators. Tabletop exercises can be as fast-moving as the crises themselves, and quick assessment of the important issues and gaps in response is critical for the success of the exercise.

4. **Use relevant, real-world scenarios.** Tailor response scenarios to your industry and the type of threats your organization actually faces. If you rarely share data with vendors, don't simulate responding to a vendor intrusion where your company and the vendor spar over who should lead the investigation and notify individuals. Think about the types of incidents your peers (and your organization) have faced in the past so the scenario feels authentic and your response personnel can take away meaningful lessons from the exercise. Similarly, use real-world examples from which to develop the scenarios—it will have a much stronger impact on the attendees. Simulate the time-crunch your company will face during an incident by highlighting required timelines for notifying relevant parties, be it the card brands (e.g., Visa, MasterCard) during a payment card incident or individuals and state regulators pursuant to state data breach notification laws. Equally important, ensure the scenario will support the specific areas you intend to test. For example, don't plan to test your network team's response protocols using a scenario geared toward an employee theft at the company.

5. **Go international.** After you've workshopped and mastered incident response at the domestic level under your various plans, incorporate international elements into your scenarios. Consider testing, if appropriate, how your company would handle an incident involving a data center located outside the United States. Bring in members from key international business lines to test your organization's response to an international incident and make sure you're prepared. As more incidents go global, global companies need to have global breach response protocols in place and need to ensure those protocols are effective through all the different types of testing.

If key personnel are reading your incident response plans for the first time only *after* an incident has occurred, even the very best drafted plans will not help your company effectively respond. By stress testing your plans before a cybersecurity incident occurs, your company will be ready (and less stressed) when the real thing hits.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey or Lou Dennig.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com