Eight Keys for Developing a Data Breach Response Plan

March 10, 2015
By Sten-Erik Hoidal

"There are two kinds of big companies in the United States... [T]hose who've been hacked... and those who don't know they've been hacked ..." – James Comey, FBI Director

It's an unfortunate fact of modern life – hacks happen. And they will continue to happen. For companies, the risks cyber security incidents pose to both business and brand cannot be underestimated. Given the sharp increase in such incidents during 2014 – up at least 50 percent, with some experts estimating as many as 42.8 million incidents – there is a growing expectation that companies have the right tools in place to respond effectively.

One of those tools is a data breach response plan. A data breach response plan is a written document that outlines a company's strategy for evaluating and responding to potential cyber security incidents. The response plan is tailored to the company's specific structures, systems and goals. And if prepared appropriately, it provides the company not only with a roadmap for handling suspected incidents, but a device for training and honing its data breach response ahead of time.

There is no one-size-fits-all data breach response plan. That said, below are eight tips for developing a response plan that is solid, efficient and functional.

1. **Identify the incident response team and their roles and responsibilities.** Ambiguity and uncertainty are impediments to breach response. This is particularly true when it comes to roles and responsibilities. To avoid ambiguity and uncertainty, identify the "incident response team" and outline the team members' roles and responsibilities in the response plan. That way, team members are quite literally "on the same page" about the scope of their duties.

2. **List strategic partners and explain the process for determining involvement.** It may be necessary in the data breach response process to involve certain strategic partners (PR firms, computer forensics experts, law enforcement, credit monitoring companies, call centers, etc.). Establish relationships with those strategic partners ahead of time. Then document the relationships in the response plan, along with an explanation of the process for determining whether the individual strategic partners need to be involved in a breach response.

3. **Outline the strategy for identifying and containing a breach.** Identifying a breach, ascertaining its size and scope, and ultimately containing the breach are all critical to an effective response. In the response plan, identify who is going to be responsible for these functions (whether incident response team members or external forensic experts) and the general steps they will follow.

4. **Explain the process for determining applicable notification requirements.** Depending on the information accessed, a breach can implicate both federal and state laws. If personally identifiable information is accessed, companies may have an obligation to provide notification to injured parties and others about the breach consistent with applicable laws. Failure to do so can expose companies to liability. Accordingly, the response plan should identify and explain the process for determining what laws and notification requirements apply to the breach.

Continued on back.

5. **Outline how notice will be provided to potentially injured parties (if necessary).** To ensure that notification to injured parties or others is provided in a prompt fashion, the response plan should outline how the notice is to be provided, who is responsible for ensuring the notification requirements are met, and the process to be followed. Consider streamlining the notification process by preparing template notices drafted consistent the most stringent notification requirements that are potentially applicable. In the event notification is required, those template notices then can be customized based on the notification requirements that are ultimately determined to apply.

6. **Develop an internal communication strategy.** Communication with boards and key stakeholders within the company about the data breach response process is essential. To that end, the response plan should explain when and how the board and key stakeholders will be informed about the breach response, as well as whether their input will be sought on major decisions during the response process. The response plan should also identify who is responsible for disseminating information and/or talking points about a breach incident to other company representatives.

7. **Develop an external communication strategy.** Depending on the type and scope of a breach, it may be necessary for a company to communicate with the media and respond to external inquiries regarding the breach. Outline the strategy for communicating with the media and responding to external inquiries in the response plan. In addition, identify who is responsible for overseeing that process and developing the external message about a breach.

8. **Describe process for deciding whether to provide assistance to injured parties.** In the event of a breach involving theft of personally identifiable information, some companies provide assistance to individuals that may have been injured by the breach – typically, fraud or credit monitoring services. Include an explanation in the response plan of the decision-making process for determining whether individuals injured by a breach will receive any type of assistance.

While this list is not exhaustive, it provides useful considerations for companies when developing their data breach response plans.