Planning for the Worst: White House Guidance on Avoiding, and Coping With, Data Breaches

The White House memo reflects changing laws and policies and provides guidance for how organizations should tailor their response plans.

Kristen Price, Haight Brown & Bonesteel, Legaltech News
May 5, 2017

The federal government is urging agencies to implement updated data breach response plans in reaction to a 27 percent increase (between 2013 and 2015) in the number of incidents in which the security of personally identifiable information (PII) has been jeopardized. PII is information used to distinguish or trace an individual's identity, i.e., Social Security numbers, birth dates, driver's license numbers, etc. Malicious hackers then use this information to execute identity theft, seek employment, obtain prescription drugs, claim benefits, etc.

To complicate things further, today's ever-changing technological landscape presents unique risks to PII collected in both the government and private sectors. In an effort to address these rapidly evolving threats, the White House set forth recommendations for the development and implementation of a comprehensive data breach response plan in a recent memorandum. While the White House memo offers guidance specific to federal agencies, it incorporates best practices from the private sector and reflects changes to developing laws and policies, providing guidance for how organizations should tailor their response plans based on the nature of their business, identity of their constituents, and the type of PII it collects and retains.

What Is a 'Data Breach' Anyway?
The term "data breach" is broad and encompasses a variety of scenarios, intentional or inadvertent, in which a person other than an authorized user accesses PII. Whether an email containing PII is inadvertently sent to the wrong person, or a third party commits a targeted attack designed to obtain PII for a nefarious purpose, a data breach response plan is essential to limiting exposure to your organization and your constituents.

In order to prevent and/or effectively respond to a breach, government and private agencies should commit to developing a breach response plan. Such a plan should be memorialized in a formal document to include "the agency's policies and procedures for reporting, investigating, and managing a breach." The memo discusses several key components to such a data breach response plan, including:

• Identifying the individuals who comprise your organization's data breach team;

• Understanding reporting requirements post-breach;
• Manners in which an agency can assess the risk of harm to individuals affected by the breach;
• Methods to mitigate the risk to individuals affected post-breach; and
• A plan to notify affected individuals.

The individuals comprising an organization's data breach response team are those persons to be convened to execute the logistics in response to a breach. The team should consist of a wide variety of organizational personnel, including IT, legal compliance, and communications staff. This may require an organization to procure specialized personnel from external sources. Depending on the size and scope of the breach, there can be both significant short-term and long-term consequences for an organization and its constituents. An established plan of who will do what and when is key to handling a breach smoothly.

A data breach response plan should identify the organizational officials responsible for notifying and consulting with law enforcement when warranted. For federal agencies, this means identifying those who will be responsible for consulting with the Office of Inspectors General and General Counsel on the agency's behalf. For private organizations, it commonly requires consultation with legal counsel who advise on state and local regulatory compliance issues. Prompt referral to law enforcement can aid in preventing additional breaches and, on occasion, can reduce the risk of harm to affected individuals.

This Seems Risky …

The risk to individuals affected by a data breach depends on the nature and sensitivity of the PII that could potentially be compromised. Certain pieces of PII are more sensitive than others. For example, Social Security numbers, driver's license numbers and bank account numbers may present an increased risk of harm to those persons whose information is breached. Depending on the nature of PII the organization collects and maintains, it may be appropriate to implement certain security safeguards to reduce the risk of harm associated with particularly sensitive data. Retaining a third-party firm to assist in this analysis and develop a digital security system consistent with the nature of the PII at risk can help avoid a breach in the first place.

If, despite safety safeguards, a breach does occur, the organization should have a plan with respect to mitigating the damage caused to affected persons, including offering guidance and services to affected constituents. Depending on the scope of the breach, it may be necessary to set up a call center operation to field inquiries from affected persons. It is now commonplace for organizations to offer advice on how to obtain a free credit report or even offer to provide identity and/or credit monitoring to affected individuals. The ability to provide these services during a time of crisis requires significant foresight and proper infrastructure, hence the necessity for a comprehensive data breach response plan.

Some breaches are minor, involving relatively mundane PII or few individuals, in which case it may not be required, or prudent, to notify all affected persons. Whether

notification is required, as well as the scope of that notification, depends on the circumstances of the breach, some being more serious than others. A data breach response plan should account for whom will notify affected individuals, timing of the notification to ensure it occurs without unreasonable delay, the contents of the notification and the method of the notification. Again, consultation with legal counsel is recommended.

Kristen Price is an attorney in Haight Brown & Bonesteel's San Diego office. She is a member of the Risk Management and Insurance Law Practice Group.