Report 2017-01 of the DHS Data Privacy and Integrity Advisory Committee on Best Practices for Notifying Affected Individuals of a Large-Scale Data Breach

Tasking

In September 2015, Department of Homeland Security (DHS) Chief Privacy Officer asked the Data Privacy and Integrity Advisory Committee to provide written guidance on best practices for notifying individuals impacted by a large-scale data breach.[1] The Committee was asked to consider and respond to four questions.

1. In the context of large-scale data breaches, what criteria should the Privacy Office consider to inform DHS's decision of whether and when to notify the impacted individuals?
2. Once DHS has decided to notify impacted individuals, what are best practices with respect to the source, content and delivery mechanism (e.g., mail, e-mail) for the notification?
3. Is it possible to "over notify" by saturating affected individuals with information or bulletins?
4. In addition to delivering the actual notification, are there best practices supporting a notification process (e.g., establishing a call center) that should he considered?

Background on Data Breach Response

Since California's data breach notification law took effect in 2003, similar laws have been passed in all but three states. While a federal law of broad application has not been enacted, there are federal breach notification laws and regulations that apply to the U.S. Department of Veterans Affairs, certain financial institutions, and the health care industry, including certain federal health care agencies. In addition, the Office of Management and Budget has issued guidance, beginning in 2007, that requires all federal agencies to implement a data breach notification policy.

Over the past decade, various entities have published policies and best practices for responding to data breaches. DHS's Privacy Incident Handling Guidance, last revised in 2012, reflects the basic structure of most data breach response guides.

- Have a written data breach response plan.
- Designate a team to coordinate the response.
- Hold desktop incident exercises to test your plan.

[1] See Appendix A.

- Develop internal notification procedures.
- Conduct an initial investigation and take risk reduction measures.
- Make the decision whether to notify.
- Notification: Identify whom to notify (potentially including law enforcement, government agencies, affected individuals); timing, method, contents and format of notice.
- Conduct final assessment (lessons learned, corrective measures and policies, changes to response plan)

Best Practice Recommendations

These best practice recommendations will not address the full spectrum of policies and actions in responding to a data breach. There are many excellent resources from government and private-sector sources. Nothing in this document negates the requirement for all agencies to comply with Federal Information Security Management Act (FISMA) requirements or with directives from the Office of Management and Budget (OMB), including M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information." Instead, the best practice recommendations here focus on the specific questions posed in the tasking letter, and may be considered as supplemental to other federal requirements.

1. Making the Decision to Notify Affected Individuals

When a data breach has been detected and confirmed, the decision on whether to notify those affected, the data subjects, may require more than a legal analysis.[2] DHS must certainly comply with laws, regulations, and official policy regarding the decision. In most cases a risk analysis is required. Note that the full facts surrounding the breach may not be initially correct and indeed may be unknowable (e.g., the possible actions of the possessor of a stolen device containing personally identifiable information or the ultimate fate of a missing data tape). Indeed, OMB M-17-12 requires agencies to "conduct and document an assessment of the risk of harm to individuals potentially affected by a breach."

In assessing the level of risk, DHS may consider a policy of allowing a "good faith employee exemption," which is provided for in 39 of the 47 state breach laws.[3] Such a provision allows for not notifying data subjects in cases where otherwise qualifying personal information has been inadvertently acquired by an employee or agent who was not authorized to access that

[2] FISMA requires agencies to report all incidents involving personally identifiable information to US-CERT, whether or not a breach is confirmed.

[3] Only Connecticut, Kansas, Mississippi, Ohio, Rhode Island, Virginia, West Virginia, and Wyoming do not have such a provision in their breach notification statutes.

information, provided that the employee or agent did not use the information or further disclose it. This situation would indicate a low level of risk of harm to the data subjects.

The risk analysis should include assessing the nature of the data, including its sensitivity (e.g., Social Security numbers, medical information) and its usability (e.g., level of encryption or other means of obfuscation). Other factors to consider include the nature of the data subjects and their vulnerability to harm from the particular data breached (e.g., law enforcement officers whose home addresses in the wrong hands could result in harm), and the nature of the threat. The analysis should also consider different types of harm, not just various forms of identity theft (e.g., reputational and dignitary harms, discrimination, and physical harm). DHS should also consider the benefits of notification, in particular whether notification would enable those affected to take defensive actions.

The analysis leading to a decision about notification must be conducted rapidly, since both legal requirements and the interests of those affected necessitate prompt notification. It is important to seek a balance between the need for speed and the need for accurate information in the notice. Factors to consider in striking such a balance include whether the breach has become public and whether it poses a risk of imminent harm to affected individuals. Another factor is the ability to determine the scope of the breach, i.e., the universe of those affected. An overly broad notification may unnecessarily alarm people who, upon further investigation, may be found not to have been affected. It may not, however, be possible to achieve perfect knowledge and a long delay in notifying can result in greater harm to more people.

2. Preparing and Delivering the Notice

The Committee provides the following best practice recommendations on preparing and delivering a breach notice. Creating a notice template, adaptable to different fact scenarios, helps to streamline the process of sending the notices. Legal and policy requirements for the notice should be consulted, but a written notice, sent by first class mail, is generally preferred. In most cases, a written notice is more likely to reach the intended recipient and less likely to be overlooked than a notice sent by email. The envelope and the contents should be designed not to look like an advertisement. There are situations in which a different delivery method may be appropriate. If the normal means of communication with the affected individuals is email, such as holders of online accounts or employees, then an email notice may be an appropriate communication method.

When postal or email addresses for those affected are not available, or when the number affected is so large as to make mailing notices infeasible, then notice may need to be made on a website. The notice should be linked to a recognizable title (e.g., “Security Incident.” Or “Data Breach Information”). Media alerts are also necessary to make people aware of the website information.

The notice should be written in plain language, avoiding legal or technical jargon. It should be in languages other than English when the recipients' language preferences are known, and the information should be communicated in a manner that maximizes accessibility.[4] The format of the notice should make it easy to read and understand, using headers to highlight the key points. For example, headers might be What Happened, What Information Was Involved, What DHS Is Doing to Help, What You Can Do, and For More Information. A means to obtain answers to questions, ideally a toll-free number, should always be provided.

The contents of the notice should be focused on the information the recipients need to have a basic understanding of what happened and to take appropriate actions to protect themselves in the specific situation. Including a lot of extraneous information, such as general information on identity theft, can obscure the basic essential points.

It is important that the notice's advice on what to do be tailored to the type of data breached.[5] For example, placing a fraud alert on credit files protects against someone using a breached Social Security number to open new credit accounts or apply for insurance, employment, or rental housing. A fraud alert does not, however, provide any protection against someone using a stolen credit card number to make charges on that account. In breaches of single account numbers, monitoring or closing the account is an effective protection.

When more than one entity was involved in the breach, such as a breach that occurred at a third-party vendor, the source of the notice (the name on the letterhead) should be the entity that is most directly known to the recipients. The signature on the notice should be of a fairly high-level person in the notifying entity, to indicate the seriousness with which the incident is regarded.

3. Concerns About "Over-Notification"

OMB M-17-12 advises agencies to "balance the need for transparency with concerns about over-notifying individuals." Over the years, as additional states enacted data breach notification laws, various parties, including the Federal Trade Commission, have expressed concern about the possibility of "over-notification," with a barrage of notices of breaches leading people to ignore the notices they receive and fail to recognize real risks of harm.[6] On the other hand, data from Javelin Strategy & Research show that while the proportion of consumers notified of data

[4] Executive Order 13166, "Improving Access to Services for Persons with Limited English Proficiency" at https://www.justice.gov/crt/federal-coordination-and-compliance-section-180 and Section 508 of The Rehabilitation Act of 1973, Related Laws and Policies at https://www.section508.gov/content/learn/laws-and-policies.

[5] Specific advice based on the type of information breached is available from the Federal Trade Commission at www.identitytheft.gov/Info-Lost-or-Stolen.

[6] Comment of Federal Trade Commission Staff to the Federal Communications Commission, In the matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, May 27, 2016, at 31-32, available at www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf..

breaches has increased over time, consumers' perception of the importance of such notices has also increased. Javelin found that breach notices were received by 10 percent of U.S. consumers in 2013, increasing to 25 percent in 2014. At the same time, the proportion of consumers who agreed that it is important to take the protective steps mentioned in a breach notice rose from 42 percent in 2013 to 54 percent in 2014.[7]

Individuals affected by a data breach are in the best position to determine the importance of a given incident and its potential for harm to them. To reduce the likelihood that individuals would become desensitized to notices, the language and format of the notice should make it easier for recipients to understand what the notice is, make an assessment of their own risk, and take appropriate action.

4. Providing Additional Support for Affected Individuals

No matter how clearly they are written and presented, most breach notices should be supplemented with additional sources of information and assistance. A call center with staff that has been appropriately trained should be available to answer questions, in multiple languages where appropriate, and should include TTY or other accessibility mechanisms. There should also be an escalation plan for handling non-routine calls. In seeking to balance promptness with accuracy in providing notification, the need to have a well-prepared call center in place should be considered. A website can also be used to provide updated information, as new facts become known and frequently asked questions are identified through the call center. Website information can also be used to verify the authenticity of a written notice.

A mitigation product that provides assistance to breach victims can be helpful, particularly in the case of breaches of Social Security numbers. Such a product should offer services that are appropriate to the nature of the incident and the breached data (e.g., credit monitoring is not relevant or helpful in payment card data breaches, but assistance in clearing up problems that could arise may be).[8] Consider social engineering risks in the communication about mitigation products.

[7] Javelin Strategy & Research, *2015 Data Breach Fraud Impact Report*, June 2015, available from Javelin at www.javelinstrategy.com.

[8] Tips on selecting a provider of an "identity theft service" mitigation product to offer breach victims are available from the Consumer Federation of America's Identity Theft Services Best Practices Working Group, at http://consumerfed.org/wp-content/uploads/2016/09/9-7-16-7-Questions-to-Ask_Fact-Sheet.pdf.