Security before and after a data breach

By Ronald I. Raether Jr.

Well, it finally happened. Information security has informed you that there has been unauthorized access to personal information despite all the protections you put in place.

You now join a group of more than 200 other companies and government agencies that have provided notices of security data breaches since February 2005. Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, http://www.privacyrights.org/ar/chrondatabreaches.htm (last visited June 30, 2006).

While the protection of sensitive personal information is important to your business and you have taken adequate steps to protect the data, as the chair of the FTC has reported to Congress: "It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." *Prepared Statement of the Federal Trade Commission Before the United States Senate Committee on Commerce, Science, and Transportation*, at 6 (June 16, 2005) (statement of Deborah Platt Majoras, chairman of the FTC).

Recognizing that no security is perfect, you are thankful that you can pull out your contingency plan prepared for just this event. You begin by organizing your quick-response team and send out the e-mail you had prepared in advance, with only slight modifications to capture the facts of the events reported to you. After your initial meeting, each member of the response team moves into action. More facts are provided, you learn where the problem locations are, and the team moves forward to comply with the notification requirements of each jurisdiction.

You have investigated the cause of the unauthorized access and have notified the appropriate regulatory authorities. Your media team has issued a press release and customer service representatives are prepared to handle inquiries from those provided notice and from the media and regulators. While the execution of every plan presents some unique or unexpected events, you learn from those experiences and the process is improved. All said and done, your planning and execution have helped your business work through a potential crisis.

It is unlikely that many of the companies that went through the notification process in 2005 had this type of experience. Most companies had not planned for how to respond to the unauthorized access of personal information or how to provide notice to affected consumers. The absence of such plans is understandable. In early 2005, only California required such notifications. Even then, it was uncertain what circumstances would trigger the requirements of the California statute.

On Feb. 15, 2005, ChoicePoint announced that approximately 145,000 people had their personal information potentially compromised after identity thieves established accounts. ChoicePoint not only notified consumers from California whose information was obtained, but also consumers in other states. *ChoicePoint: More ID Theft Warnings*, Feb. 17, 2005, http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/index.htm.

After the ChoicePoint announcement, state legislatures moved on the notification issue. While no federal statutes exist yet, at least 34 states have passed laws that require consumers to be notified when their personal information has been compromised. Ronald I. Raether Jr. & Michael Lamb, *Significant Developments in Computer and Cyberspace Law*, at 3-11 to -20 (June 9, 2006), http://www.ficlaw.com/newsframe.html. As a result, today there are plenty of reasons to develop a breach notification plan.

This article provides the basic building blocks for development of a breach notification plan. The starting point is to understand the applicable laws and variations among existing state statutes.

The natural place to begin is California's breach notification statute. In 2002, California became the first state to enact legislation directed toward notification after a security data breach. Cal. Civ. Code § 1798.29 (Deering 2006). The California law, commonly known as Senate Bill 1386, requires companies that store personal information data electronically to notify California consumers of a security breach if the company knows or reasonably believes that unencrypted information about the consumer has been subject to a security data breach.

One of the most significant privacy laws to have been enacted in years, Senate Bill 1386 required ChoicePoint to provide security breach notifications. It was ChoicePoint's announcement that began the chain of events that caused at

Raether is a partner at Faruki Ireland & Cox PLL, in Dayton, Ohio. His e-mail is rraether@ficlaw.com.

ing an understanding of all the laws that may apply should a breach notification plan be developed. While the complexity of the plan will vary depending on the size and nature of the business and uses of protected information by the company, a good plan includes four basic elements: (1) a dedicated incident response team; (2) an initial assessment plan; (3) a notification plan; and (4) an internal and external communication plan.

The breach notification plan should identify the members of the response team, who also should be involved in the development of the plan. An effective team includes the chief privacy officer or chief security officer (or their equivalents), a representative from the business unit from which the data was accessed, legal (either in-house or outside) counsel, and a public relations coordinator. It is important to include in the initial assessment plan a communication protocol to notify the team when an incident occurs and to establish a timeline and list of action items for an initial assessment and subsequent steps as deemed necessary.

A valuable initial assessment plan includes: (1) an investigation of the incident conducted under the direction of legal counsel; (2) a process to identify and execute corrective measures to prevent exploitation of the discovered vulnerability (such as plug the hole that was used to gain access to the data); (3) an assessment of the type of data and its origin to identify applicable law; (4) an assessment of the facts to determine whether notifications are required; and (5) a process to implement the notification and communication plans discussed further below.

In addition to having a plan to assess the incident quickly, the company should be prepared to provide the notifications required by the applicable statutes. An effective notification plan includes written correspondence drafted in anticipation of having to provide notice to consumers, and some thought should be given as to who will be the sender. While some circumstances may justify the letter coming from the CEO or head of the business unit at issue, it may be preferable to have the chief security officer send the notice letter. Regardless, the sender or his or her organization will need to be prepared to respond to government and consumer inquiries likely to follow.

The company should think through how the notifications will be delivered. Most states require the notice to be sent by first-class mail. Some provide for substitute notice methods; for example, Pennsylvania allows e-mails to be used where a prior relationship existed and the company has a valid e-mail address. Other states, such as Connecticut, permit notice by phone. In most circumstances, the preferred method will be first-class mail.

Depending on the resources of the company and the number of consumers affected, the notices might be sent by a third-party vendor or in-house using the resources of the marketing department. A system should be created to track communications that are returned as undeliverable. In such circumstances, and possibly initially depending on the data available to the company, third-party resources may be needed to find a valid address or phone number for the consumer.

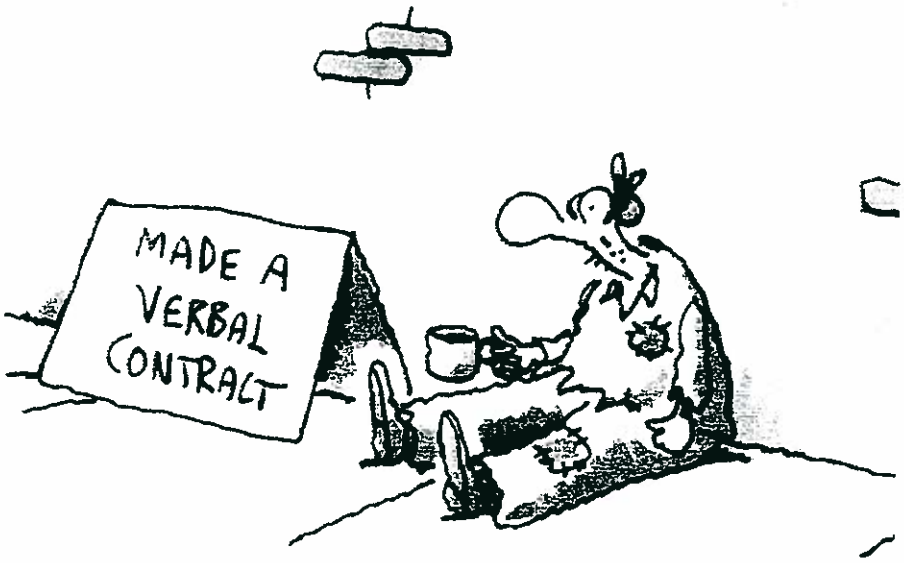
Many statutes require specified government agencies to be notified in the event of a breach. Even if not required, the company may decide to provide such notice for various reasons. For example, while not required by applicable law, the company may decide to notify a regulator with whom the company deals with regularly to avoid misunderstandings that might develop by receiving incomplete information from indirect channels.

When contacting government agencies, a pre-drafted letter may not be the best tactic. Instead, a telephone call or in-person contact may be more desirable, especially if the company has an established relationship with someone within that agency.

An effective communication plan includes a Web page to provide information about the incident to consumers, government agencies, and the general public. Much of the design and coding of the Web page should be part of the breach notification plan. Initial design of the Web page ahead of a possible breach allows for it to be developed in a more deliberate manner and saves valuable time and resources for other important tasks.

As part of the notification plan, the company also should identify a menu of resources that could be made available to the notified consumers. Many companies involved in breach notifications have wisely provided free credit reports, identity theft protection, credit monitoring services, and identity theft counseling where appropriate.

Developing relationships with vendors and defining protocols prior to any incident is important to help avoid miscommunications and unnecessary mistakes. The company may want to track the number of consumers who accept



least 34 states to enact statutes that require notification to a person whose personal information (electronically stored) was accessed by another person or business without authorization. Many of these statutes are based, in large part, on California's Senate bill.

To determine whether the breach notification statute applies, a company should first identify the type of information it has. The company should then compare the list against what personal information is protected by applicable statutes. Many states define "protected information" similarly to include a combination of personal identifiable information (such as name or address) with (1) Social Security number; (2) driver's license number or state identification number; or (3) account number in combination with a security code or password. See, for example, Cal. Civ. Code § 1798.29(e)(1)-(3) (Deering 2006).

Some states, however, have expanded the definition of protected information to include other types of data. The chart above identifies some of these variations:

State	Arkansas	North Carolina	North Dakota	Wisconsin
PIN code		✔		
Medical information	✔			
DNA				✔
Mother's maiden name			✔	
Employee number			✔	
Digitized or electronic signature		✔		
Biometric data		✔		✔

In addition, many states include exceptions to the general notification requirement, such as when the data was encrypted. Similarly, most states provide exception where the data was gathered from a publicly available source. However, states such as Arkansas, Rhode Island and Utah have a far more limited exception.

With the exception of states such as Illinois, most statutes expressly permit (or require) some delay before sending notifications to consumers to allow law enforcement a reasonable amount of time to conduct an investigation. Other states require that the notifications be sent within a prescribed period of time after the unauthorized access is discovered. See, for example, Florida (Fla. Stat. Ch. 817.5681(10)(a)) and Ohio (Ohio Rev. Code § 1349.19(D)). A good notification breach plan should include a matrix of the applicable state statutes and their requirements.

Understanding pending federal bills also is important. While numerous bills are under consideration in Congress, this article focuses on a more recent bill that includes many of the elements being considered by Congress. With this foundation in place, this article will discuss some common features that should be included in a breach notification plan.

While Congress has considered several bills that in some way deal with data security and breach notification, none have made it to a floor vote in either chamber. The most recent bill, introduced on June 26, 2006, provides a good example of the elements being considered by Congress.

The Data Security Act of 2006, S. 3568, would create a uniform national standard to require notification if "sensitive account information or sensitive personal information involved in a breach of data security is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumer." Library of Congress THOMAS, http://thomas.loc.gov/cgi-bin/query/z?c109:S.3506.IS. S. 3568 expressly references the standard being applied to other breach notification statutes, namely that unauthorized access is not enough to trigger notifications. Instead, the intruder must have a type of data and the means to commit identity theft or to engage in fraudulent financial transactions.

Like the state statutes, S. 3568 exempts information available from public records. In addition to notifying the affected consumer, S. 3568 requires notification of: (1) the Federal Trade Commission, state attorneys general, and other government agencies that regulate the data or company's business; (2) the appropriate law enforcement agency; (3) entities that own or were the source of the data; and (4) if more than 5,000 consumers' data are exposed, nationwide consumer reporting agencies.

In sum, the pending federal legislation provides further guidance into what should be included in a breach notification plan, such as the requirement of S. 3568 that the company conduct an evaluation of the cause of the breach and implement corrective action based on those findings. Notification of regulatory agencies, law enforcement, and consumer reporting agencies, while not required by all existing state statutes, is another guiding principle from S. 3568 that should be included in a breach notification plan.

While the above summary is a general review of the applicable law, a comprehensive review of the law is an important component of developing a breach notification plan. Only after gain-

the free services or who identify anomalies in their credit reports. Planning ahead will help improve the likelihood of being able to track such data and improve accuracy.

The announcement of a data breach will attract public attention, as well as elicit inquiries from the affected consumers. As part of a communication plan, a dedicated telephone number should be established to respond to such inquiries. To avoid miscommunications, staff the dedicated number with employees who are trained to deal with data security and who have a prior understanding of the company's breach notification plan.

An effective communication plan includes a standard set of frequently asked questions with proposed responses. These FAQs can be made available to the staff and posted on the company's Web site. A press release should be drafted and a principal spokesperson identified and designated as the sole contact for addressing inquiries from the media. Corporate communications must educate all points of interaction with the public and customers, such as customer service representatives and the sales force, to direct inquiries to the dedicated number or the identified spokesperson.

Not all issues will necessarily be addressed in the communication plan. On learning the facts of the particular incident, the project leader reviews all documents drafted as part of the breach notification plan and modifies the plan to address the specific circumstances of the incident. The notice team reviews the timetable and action items to ensure that the specifics of the incident justify a press release or many of the other action items identified above.

As with all communications (electronic or otherwise), the public relations department is prepared for public scrutiny of every statement and phrase used. In addition, as ChoicePoint and even the Department of Veterans Affairs have learned, litigation often follows on the heels of a data breach notification. The company must determine whether counsel from lawyers that specialize in such litigation should be involved in the planning and implementation of the breach notification plan.

Throughout the incident response and again at the conclusion, the company should evaluate its information security program. While the initial assessment addresses immediate threats, a deeper analysis should occur to determine whether more systemic issues are present. For example, was there a gap in the development process that created the vulnerability? While the immediate action in this example might be to fix the network configuration or coding error, the long-term action might be to require additional testing or to increase the involvement of the security officer in product development.

After the crisis has passed, the breach notification team evaluates the breach notification plan itself to identify what worked, what did not, and to determine how the plan should be improved. Even if no incidents occur, the breach notification team periodically reviews and updates the plan to adjust to the ever-changing legal landscape and likely security threats.

The above steps are a useful guide to begin the process of developing a breach notification plan. However, even if faced with a breach incident without a plan, the above steps can help guide the process to make sure critical elements are considered. As each company is unique in its products, use of technology, operations and countless other variables, these steps will need to be customized and thought must be given as to how to use these concepts.

By being proactive and developing a breach notification plan *before* an incident occurs, a company can be more deliberate in making thoughtful decisions and can react more swiftly to a potential crisis.

Statement of Ownership, Management, and Circulation

(Act of August 12, 1970: Section 3685, Title 39, U.S. Code)
1. Title of publication: *Business Law Today* (ISSN: 1059-9436)
2. Publication No.: 014-567
3. Date of filing: 10-1-06
4. Frequency of issue: Six times a year
5. Number of issues published annually: 6 (six)
6. Annual subscription price: $14.00
7. Location of known office of publication: 321 North Clark Street, Chicago, IL 60610-4714. Contact Person: Ronald F. Kadlec, (312)988-6310
8. Location of headquarters or general business offices of the publisher: American Bar Association, 321 North Clark Street, Chicago, IL 60610-4714
9. Names and addresses of publisher and editor: Publisher: American Bar Association, 321 N. Lake Shore Drive, Chicago, IL 60610-4497; Editor: Kathleen Hopkins, Real Property Law Group PLLC, 1218 Third Avenue, Suite 1900, Seattle, WA 9801
10. Owner: American Bar Association, 321 N. Lake Shore Drive, Chicago, IL 60610-4714
11. Known bondholders, mortgagees and other security holders owning or holding 1 percent or more of total amount of bonds, mortgages or other securities: none.
12. For completion by nonprofit organizations authorized to mail at special rates (Section 132.122 Postal Service Manual): The purpose, function and nonprofit status of this organization and the exempt status for federal income tax purposes has not changed during the preceding 12 months.
13. Publication name: *Business Law Today*
14. Issue date for circulation data below: July/August 2006, Volume 15, No. 6.
15. Extent and nature of circulation: *(See column 1: Average number of copies each issue during preceding 12 months. Column 2: Actual number of copies of single issue published nearest to filing date.)*

		Column 1	*Column 2*
A.	Total no. copies printed	52,593	51,600
B.	Paid circulation		
	1. Paid or requested mail subscriptions stated on Form 3541 *(include advertiser's proof and exchange copies)*	38,843	35,939
2.	Paid In-County Subscriptions Stated on Form 3541 *(include advertiser's proof and exchange copies)*	0	0
3.	Sales through dealers and carriers, street vendors and counter sales and other Non-UPS Paid Distribution	0	0
4.	Other Classes Mailed Through the USPS	0	0
C.	Total paid and/or requested circulation *(Sum of 15b. (1),(2),(3),and (4))*	38,843	35,939
D.	Free distribution by mail, samples, complimentary and other free copies		
	1. Outside-County as Stated on form 3541	7,392	9,281
	2. In-County as stated on Form 3541	0	0
	3. Other classes mailed through the USPS	0	0
E.	Free distribution outside the mail *(carriers or other means)*	0	0
F.	Total free distribution (sum of 15D and 15E)	7,392	9,281
G.	Total distribution (sum of 15C and 15F)	46,235	45,220
H.	Copies not distributed	5,345	5,027
I.	Total (sum of 15G and 15H)	52,593	51,600
Percent paid and/or requested circulation		84%	79%

16. This Statement of Ownership will be printed in the Nov/Dec 2006 issue of this publication.
17. I certify that all information on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties). (Signed) Bryan Kay, Director ABA Publishing.