

# Security Breaches: Notification, Treatment, and Prevention

A computer containing sensitive, personal information (name, social security number, driver's license number, debit or credit card number, etc.) is compromised by a security breach. An examination of system logs is inconclusive as to whether or not the sensitive data was accessed by the intruder. The risk for identity theft is unknown but probably low. This situation, not uncommon for many colleges and universities, presents both ethical and legal quandaries for campus administrators. Should they notify the individuals whose personal information may—or may not—be in the possession of an unauthorized person? In other words, how should they treat this “disease”—the bleeding of personal data—currently plaguing higher education?

## Notification

Regardless of the ethical issues, the criteria by which notification decisions are made may soon be established by federal or state law. California Civil Code 1798 (commonly known as California Senate Bill 1386 or SB1386) has forced colleges and universities in the state of California to report incidents, possibly at higher rates than they might have done in the absence of a legal requirement to notify citizens. Likewise, several other state legislatures, noticing the trend for security breaches within commercial data brokers (e.g., ChoicePoint, LexisNexis) and following the lead of California, have proposed their own variations of SB1386 in an effort to protect their citizens. Finally, Senator Dianne Feinstein (D-Calif) is determined to create a national standard for data notification. In April 2005, Senator

Feinstein introduced S. 751, known as the “Notification of Risk to Personal Data Act.” She announced, “We desperately need a strong national standard that says whenever a data system is breached, everyone who is at risk of identity theft must be notified.”<sup>1</sup>

Although S. 751 is based on SB1386, Senator Feinstein points to the following provisions that make the proposed act even stronger than the California law:

- It covers both electronic and nonelectronic data.
- It includes encrypted as well as nonencrypted data.
- It closes the “loophole” that allows companies to follow weaker notification requirements.
- It lays out specific requirements for what must be included in notices.
- It has tougher penalties.

Whether or not S. 751 becomes law in this Congress, the provisions are worth noting, especially in the likely event that state legislatures continue to introduce disparate versions of security notification bills. Some of the changes from the California law could negatively affect colleges and universities. For example, in S. 751, the threshold cost that would permit “substitute notice” (meaning a conspicuous posting on the organization's Internet Web site and notification to major print and broadcast media) is increased from \$250,000 to \$500,000. Additionally, the content of the notification would require the establishment of a toll-free number, something that may be costly and difficult to do, especially for smaller colleges.

The California law's “loophole” that Senator Feinstein referred to is a “safe harbor” for organizations “that maintain [their] own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements.”<sup>2</sup> This provision would permit an organization to establish a more flexible determination of when a “substitute notice” is acceptable. Determining the threshold for when to report a security breach is a difficult decision, although the University of California has provided its institutions with some guidance, as has the Office of Privacy Protection in the California Department of Consumer Affairs.<sup>3</sup>

Another consideration for data security and incident notification is the evolving standards of legal liability. There is much speculation that negligence principles (which impose liability under common law for failure to fulfill a legally recognized duty) will be applied to organizations that are charged with safeguarding personal information. The Michigan Court of Appeals recently signaled the potential for identity theft lawsuits being pursued as negligence claims. In *Bell et al. vs. Michigan Council of AFSCME et al.*, the court upheld a jury award of \$275,000, finding that the defendants owed the plaintiffs a duty when the defendants failed to safeguard personnel information and their negligence facilitated identity theft perpetrated by a third party.

Although this case involved personal information that was probably obtained in paper versus electronic form, the court was unequivocal about the importance of “procedures or safeguards . . . to ensure

that confidential information was not accessed by unauthorized persons.” The court denied that it was creating a new tort of “identity theft negligence” but concluded: “That the Legislature has recognized the need for specific laws addressing the growing problem of identity theft and has recently enacted legislation, only strengthens our view that imposition of a duty is appropriate in this case.”<sup>4</sup>

## Treatment

Given the momentum toward state or federal requirements for incident notification and the likelihood of liability (either through statutory fines or common-law negligence claims) for data security incidents, what is an institution to do? Senator Feinstein’s bill can be viewed as a set of commonsense practices that, when used to “treat” the security breach, are likely to keep the institution in compliance with legal requirements and possibly limit liability. In summary, her approach is as follows:

- Following the discovery or notification of a security breach of “personal information” (likely defined to include name, social security number, driver’s license number, credit card number, etc.), the institution should notify individuals whose personal information was acquired (or reasonably believed to have been acquired) by an unauthorized person.
- Notification should be prompt, without unreasonable delay, following the discovery of the breach and after taking appropriate measures to determine the scope of the breach and to restore the integrity of the data system.
- The notification should be in writing, sent via traditional means, sent by e-mail, or posted on the Internet site of the institution. (Note: the use of “substitute notices,” such as posting the notice on the Internet site under SB1386 or Senator Feinstein’s bill, may require that an institution meet certain minimum thresholds before it can resort to this less-costly means of notification.)
- The notification should contain a description of the categories of information acquired by an unauthorized person and should possibly include a toll-free number for contacting the in-

stitution or for learning more about the incident, as well as the toll-free contact telephone numbers and addresses for the major credit-reporting agencies.

## Prevention

The recent focus on laws that would require security breach notifications—and the corresponding expenditure of resources and energy—may be overshadowing the underlying causes of the “disease,” along with the precautions that could enhance data security in the first place. The following recommended practices are important preventative strategies.

*Eliminate the use of Social Security numbers as primary identifiers.* The exposure of Social Security numbers (SSNs) as part of a security breach will typically trigger a decision to notify. Limiting the reliance on and use of SSNs will greatly minimize risks. Several states have regulated the use of SSNs, and several bills have been introduced in Congress to limit the use of SSNs. If storage of SSNs or other personal information on laptops or personal computers is necessary, the data should be encrypted or a password should be required for access.

*Establish privacy policies and promote fair information practices.* Information-collection practices across the institution need to be inventoried. Fair information practices (including the principles of notification; minimization; secondary use; nondisclosure and consent; need to know; data accuracy; inspection and review; information security, integrity, and accountability; and education) should be established and promoted. A privacy statement should inform all individuals from whom information is collected of the institution’s privacy policies and practices.

*Conduct a security risk assessment and analysis.* In highly distributed campus environments, sensitive data and personal information can reside in multiple locations. Identifying the location of personal information and establishing classifications that differentiate public information from personal information will help an institution develop a plan for the appropriate protection of information assets. Once the information assets have

been located and categorized, a risk assessment should be conducted to identify the corresponding threats and vulnerabilities. A prioritized plan should outline how threats and vulnerabilities will be mitigated.

*Develop incident-response procedures and protocols.* Ideally, the question of whether or not to notify will have been previously rehearsed and dictated as part of an overall incident-response plan. The establishment of policies, procedures, and protocols for the handling of data security incidents will pay off when crisis mode sets in. However, once the policies and procedures are established, they need to be followed, lest the institution create an additional source of liability.



Although recent leaks of data from college and university computer systems have caused quite a stir in the news, there is no authoritative data to suggest that the number of security incidents is on the rise. But the publicity and the resulting emphasis on possible legal requirements are causing more colleges and universities to treat the problem by notifying individuals that a system compromise has occurred. In addition, institutions should be looking to prevention—that is, how to prevent and detect data security incidents in the first place. Used together, the appropriate treatment and preventative measures could, in the future, cure the security breach disease.

## Notes

1. “Senator Feinstein to Introduce Tougher ID Theft Notification Bill,” press release, April 11, 2005, <<http://feinstein.senate.gov/05releases/r-notification411.pdf>>.
2. California Civil Code 1798.29(h).
3. University of California Office of the President, “Determining the Threshold for Security Breach Notification,” November 25, 2003, <[http://www.ucop.edu/irc/itsec/security\\_breach\\_notification.pdf](http://www.ucop.edu/irc/itsec/security_breach_notification.pdf)>; Office of Privacy Protection, California Department of Consumer Affairs, “Recommended Practices on Notification of Security Breach Involving Personal Information,” October 10, 2003, <<http://www.privacy.ca.gov/recommendations/secbreach.pdf>>.
4. State of Michigan Court of Appeals, unpublished opinion, February 15, 2005, no. 246684, Wayne Circuit Court, LC No. 01-107819-NO, <<http://www.michbar.org/opinions/appeals/2005/021505/26184.pdf>>.

**Rodney Petersen is Policy Analyst and Security Task Force Coordinator at EDUCAUSE.**