Dealing with Data Privacy Regulations and SB-1386

By Arshad Noor
arshad.noor@strongauth.com

Disclaimer: Nothing in this article should be construed as legal advice. If you want a legal opinion, please consult with your lawyers.

With the dramatic rise of identity theft[1], the United States is witnessing an unprecedented passage of laws focused on data privacy, something that our EU colleagues are probably more familiar with. The Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) are industry-specific federal regulations that establish broad rules regarding information privacy in the healthcare and the financial sectors, respectively.

However, a little-known law from California—Senate Bill 1386, or SB-1386[2]—is more likely to cause the equivalent of an earthquake across all industries. That is because of its specificity and the consequences for not having the right defenses, and I don't just mean technology defenses. This article provides more information on SB-1386 and what you can do to help your company build those defenses.

SB-1386

SB-1386 was passed unanimously in September 2002 by the California Legislature and Senate as the result of a hacking attempt on the Teale Data Center, the data center for the government of California. The hackers apparently gained and had access to confidential information on every California government employee and elected official for over six weeks, while the individuals affected were kept uninformed. The investigation still continues.

As a result, the law, effective July 1, 2003, requires any organization that stores confidential information about a California resident on a computerized system, to notify those individuals immediately upon the discovery of a breach to that computer system. Confidential information, according to the statute, is defined as Social Security numbers (unique identification numbers that underlie all important transactions of a person living in the United States), California drivers license number, California identification card number (a non-mandatory identification card), account numbers, credit or debit card numbers.

It does not matter where you operate from, where you store the computer data or who breaches the information; it doesn't even matter whether the information was actually stolen or not (which is difficult to prove, in any case, unless you have sophisticated devices and controls). As long as the computer system storing that confidential data was breached, the company has a responsibility to notify those individuals. The only exception to immediate notification can be provided by a law enforcement agency, if it determines that disclosure might hamper its investigation. However, the disclosure may still be required upon the conclusion of the investigation, so a company must be prepared to disclose, regardless of the outcome of the investigation.

The most significant part of the law comes from the fact that non-compliance does not just result in civil fines by the government—equivalent to a slap on the wrist. The law permits affected Californians to bring about a class-action lawsuit against the company and recover damages, in addition to all other remedies available by law. Given the dramatic rise[3] of computer incidents over the last 3 years, the litigious nature of American consumers and the large judgments awarded by juries, it's only a matter of time before the lawyers in California start getting busy.

Unfortunately there is no "safe harbor." Having firewalls, virus scanners, an intrusion detection system, two-factor authentication systems, etc. are insufficient evidence of a company doing what it can to protect confidential data. These tools cannot prevent compromises by unauthorized insiders—(employees, contractors, consultants, partners, etc.) or by an unauthorized outsider who has compromised the network identity of an authorized insider.

The kinds of defenses required to minimize damages are very different from the usual countermeasures, since the company must now prove that it had complete control over the confidential data when the breach occurred. Anything less would be indicative of a management that has little regard for the security of the data, or the law itself, and may be sufficient to convince a jury of negligence.

Short-term countermeasures

What must a company do to prepare for SB-1386? In addition to all the countermeasures that the InfoSec community is familiar with, there are four others it must implement in the short term, to bolster its defenses. These are:

1. A Policy on Sensitive Data Management: While every knowledgeable company has information protection, computer usage, privacy and other security policies, a sensitive data management policy is different, in that it specifically defines what the company must do in the event of a breach to computer systems and the compromise of confidential data. This policy must spell out the following components:

    1) Ownership and responsibility for the policy
    2) Functional roles required to implement the policy
    3) Responsibilities of the functional roles
    4) Procedures required to implement the policy
    5) Controls required to measure

compliance and effectiveness
6) Consequences to company insiders of non-compliance
7) Reporting requirements

2. Detailed procedures: Companies have never had to deal with mandated disclosure before; many do not even have policies about reporting breaches to law enforcement agencies, let alone procedures for doing so. To ensure compliance to the law, companies will now have to establish detailed procedures for the following:

1) Reporting sensitive data
2) Reporting breaches (internally)
3) Reporting breaches to law enforcement
4) Breach investigation management
5) Disclosure management
6) Audits

3. Measurement and Reporting Controls: Policies and procedures are meaningless if the company does not have the appropriate tools to measure compliance and effectiveness. Companies must establish controls, appropriate for their size and complexity, that give them answers to the following questions. If a company cannot definitively answer these questions in the "discovery" phase of a lawsuit, it's difficult to see how the defense can justify that they actually have a handle on the problem:

1) Where is the sensitive data?
2) Who controls it?
3) Who, and what has access to it?
4) How is it stored?
5) How is it protected?
6) Did it get breached?
7) If so, when and how?
8) What were the results of the investigation?
9) Is a disclosure required?
10) If so, how is the company handling the process to ensure compliance with the law?
11) What measures has the company taken to ensure non-recurrence of previous breaches?

4. Education: Companies now need to not only educate employees on the importance of protecting data, but must also focus on training them to recognize signs of breaches to their computers. One of the last things that a company wants to discover is that their confidential data has been available on the "net" for some time, from newspaper or television reports. Disclosure in such a situation is redundant. What's more problematic, however, is that a public "disclosure" of this kind puts additional pressure on a company. How? The company now has the burden of proving in any lawsuit brought against it that it didn't already know about the breach, and if it did, that it was exempted from disclosure by a law enforcement agency at the time the news report appeared in the press.

Recognize that the above four measures will only help you with the process of managing compliance, and in helping to reduce your exposure to damages in potential lawsuits resulting from breaches. The measures will neither make you compliant with the law, nor eliminate lawsuits in and of themselves. They are mere tools to help organize the process for the busy InfoSec professional.

Longer-term solutions

Given that California generally leads the nation in such laws, it's only a matter of time before other states start adopting similar measures. Until a uniform federal law supersedes state laws, there is the possibility of a variety of state laws, creating a regulatory nightmare for companies.

One strategy that can help minimize frequent disruptions to this management process, and one that can potentially generate goodwill among customers and employees, is to apply these practices to all customers and employees, as opposed to just California customers and employees. Should other states pass such laws, as long as they're not more stringent than the California law, you will need to do absolutely nothing to comply with the new laws other than just become aware of it. If another states' requirements turn out to be more stringent than the one you're already using, start using the more stringent process for all jurisdictions. This way, you'll never have to use more than a single policy and process at any given time, thereby making your compliance management process easier in the long run.

Another strategy to consider is to look at your existing infrastructure—platforms, architecture and technologies—and rank them based on the probability of their getting breached—from the highest to lowest. While your own experience will give you a fair indication, the CERT/CC site referenced in this article can give you empirical data. You might want to include a few technologies, platforms and architectures that you don't currently have within your infrastructure, as part of the analysis, to get a more balanced perspective.

Next, determine what it's costing you to deal with the security of these components—the Security Cost of Ownership (SCO), if you will. You should take all factors into account—the number and frequency of incidents, the cost of patching, monitoring, damage control, breach investigations, disclosures, etc.

Finally, determine what it would cost you to migrate those components to the technology, platform or architecture where the risks and costs fall below your pain threshold. You may discover that killing a few sacred cows will actually save your company a fair amount of money and make your job easier in the long term.

Conclusion

Identity theft is acknowledged to be the fastest growing crime in the United States. As laws increasingly focus on data protection, the InfoSec community is going to come under heavy scrutiny about the way it manages its function, each time a breach is widely publicized. While security budgets will almost certainly increase once the first few lawsuits are filed, unless you're willing to gamble that you're not going to be among the first few, the time to start changing is now.

Arshad Noor is the founder & CEO of StrongAuth, Inc., a Silicon Valley company that's focused on identity management and SB-1386 related solutions. He started his career on the business side 24 years ago and switched to the IT field. He has worked in the IT departments of the Port Authority of NY & NJ, New York Life Insurance Company, BASF Corporation, Citibank and Sun Microsystems, Inc. over the last 18 years. He assisted many of Sun's customers while in the Sun Professional Services group, with issues similar to those described in this article. Just before he founded StrongAuth, Inc., he built SunPKI–Sun's worldwide Public Key Infrastructure for their internal use. He can be reached at arshad.noor@strongauth.com.

[1]Federal Trade Commission Report on National and State Trends in Fraud and Identity Theft - http://www.consumer.gov/sentinel/trends.htm
[2]StrongAuth, Inc.'s SB-1386 Resource Center - http://www.strongauth.com/sb1386/
[3]CERT/CC Statistics - http://www.cert.org/stats/