GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

California's "Notice of Security Breach" What's it all About and What it Means to You

GIAC Security Essentials (GSEC)
Practical Assignment

Version 1.4b option 1

Vicki S. Harris

January 15, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract....3
Why Senate Bill 1386 was created....3
Summary of the law....3
Ways to ensure compliance....4
Recent cases involving SB 1386....5
What consumers should do if notified of an information breach?....6
SB 1386, which products or services can help?....7
Ways to ensure compliance....8
SB 1386 has a new name “Notice of Security Breach”....10
Conclusions....10
List of References....11

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper will address the recently passed Senate Bill 1386, the California Security and Privacy law. I will present a summary and provide background information on how the law was developed and adopted. Other laws that are being developed that provide additional support or enforcement for the Senate Bill 1386 will also be detailed. Examples of incidents that have required the enactment of the new law will be provided. Methods on how businesses can comply with the new law will be explained in detail. Ways that Senate Bill 1386 could affect individuals will be discussed, and how to ensure companies that are housing individuals personal data are striving for and obtaining compliance. Finally, the new name for the Senate Bill 1386 will be discussed, along with recommendations on ways to be prepared for the enforcement of the new law.

Why Senate Bill 1386 was created

California Senate Bill (SB) 1386 was first introduced by Senator Steve Peace on February 12, 2002. It was amended by the Senate in March and then made its way through the Assembly, being amended seven times before being passed in September 2002. The law officially became effective July 1, 2003 after being supported by then California Governor Gray Davis. SB 1386 was prompted by a computer hacking case which involved the theft of personal information of 265,000 California state employees (Murray). The hacker accessed the payroll department computers that held the Social Security numbers, names and salary information for state employees. It's estimated that it took nearly two months before the state employees were notified that a hacker may have accessed their personal information. Because of this incident and the delay in notifying the affected employees, California lawmakers were prompted to create a law that would ensure companies properly protect customer and employee personal data, and provide notification to all affected parties in the situation of unauthorized access to this data (Hulme, p.1).

Summary of the law

The summary of the bill is defined as any state agency, person or business owning or licensing computerized data systems that conducts business in California or if their customers reside there to expediently notify individuals whose sensitive personal information might reasonably have been accessed by an unauthorized person. Sensitive personal information is defined as a persons first and last name, along with one or more of the following: driver's licenses number, social security number; or an account, credit or debit card number with the necessary code or password that would allow access to the account (Peace, p.1). This bill does not, however, take into affect or protect other personal items such as ethnicity, political and religious affiliation, and sexual orientation. Although there are currently other bills being introduced to protect these items from disclosure, they have not passed at the national level at this time.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The bill requires the “disclosure to be made in the most expedient time frame possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures needed to determine the scope of the breach and restore the integrity of the system.”(Peace, p.3) This bill also requires those that maintain computer systems that contain personal information, but do not actually own the data or the system, to notify the owner of the system/data as soon as they know of the breach to the system. However, this notification can be delayed if it is determined by a law enforcement organization that the notification will impair the criminal investigation. While the business or owner has to comply with notifying the persons whose data was comprised, they can create and utilize their own notification process or procedure, as long as they meet the bills requirements. These requirements are dictated as one of three methods; written notice, electronic notice or substitute notice. The types of substitute notices include: email notice, placing the notice on the notifier’s website, and publication in state and local media. The business or owner can only use the substitute notice if supplying the notice will cost over $250,000 or over 500,000 notices would have to be sent (Hulme, p.1).

Ways to ensure compliance

While many businesses will not have adequate security processes or structure in place to comply with SB 1386 there are methods and means by which they can achieve the goals of SB 1386. Some businesses may believe they do not have to comply with the new law because they do not have offices in California. If they have access to or store any information in an electronic medium about an employee or customer that resides in California, they must comply. “One of the safe harbors is to encrypt sensitive data on storage media.”, so states Michael Overly a partner at Foley & Lardner, a Los Angeles law firm (Vijayan, p.2). However, just because a company encrypts the data does not guarantee an exemption. This is because there are many different types of encryption technologies available today and the company must choose appropriately. There are some types of encryption that would require only a short time to break the algorithm and there are others that could take an indefinite time frame to break the code. If the encryption technique is considered weak or insufficient for the data it is protecting, then the company still could be held liable for the exposure of the data under SB 1386 (Poulsen, p.1-2). Data classified as non-sensitive would not need to be encrypted to comply with the law; however this could create issues on how to separate data deemed as sensitive and data deemed as non-sensitive. SB 1386 does not specifically state that strong encryption must be used, but if the perpetrator is able to break the code and the encryption did not protect the data, the company could be held liable. Also, if the company does decide to encrypt sensitive data they must ensure that all copies of the information are encrypted. If the data is stored unencrypted anywhere, whether it be a laptop or a database, then security best practices are not upheld and the company could be held liable for personal information that is breached. This is a very common practice among companies not to encrypt data in all

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

locations. Another way to prevent information from being stolen is simply not to store or maintain unnecessary information about customers after its useful life. While this may seem simplistic, many companies do not purge or review information that may not be needed and thus increases their liabilities for information that is outdated or unnecessary. One reason for this is that many companies do not take the time or effort to classify the data they are maintaining, thus placing the company at risk for this type of liability. It must be noted that even with the strongest encryption on the necessary information; there is always the chance that a disgruntled or untrained employee may release or breach the customer information, thus causing a reportable incident to occur.

Throughout my information security career I have had the opportunity to perform vendor readiness for many different vendors. These vendors range from billion dollar corporations to small regional companies and I have discovered that data is not consistently encrypted across all mediums. The vendor may require sensitive email to be encrypted, but data is not stored encrypted or data is not transmitted over their internal network encrypted. With this bill, companies will need to revisit their encryption policies or risk costly lawsuits. As I have the opportunity to review different vendors/companies and their security postures since the passage of this bill, I will alert them to their required support and compliance to this new bill. Companies that do not adhere to the requirements of SB 1386 will be requested to provide mitigation to address the risk associated with non-compliance for their own protection as well as the customer's information they are maintaining.

While the California law does not spell out the actions that a company would need to take to protect themselves from non-compliance, it does insinuate that companies need methods for monitoring, detecting and responding to incidents and data breaches (Vijayan, p.1). To implement these types of methods, a policy would be written to ensure the roles and responsibilities of those tasked with such duties and that they have an understanding of the goals for compliance with SB 1386. This would include what types of sensitive data is stored and how, who owns it and has access to the data, and how it is protected. Also, they will need to ensure that the necessary executive management and legal entities within the organization review and support ownership of the policies.

Recent cases involving SB 1386

While this bill has only recently passed and there have been few lawsuits regarding the failure to comply with this bill, one can speculate on the legal and financial liabilities that companies may face. The notification fees alone for a large corporation that had a breach could place them in financial ruins. Notwithstanding the civil lawsuits and legal fees that would come along with the case, a company's reputation to the public and shareholders could be irreparably damaged. If the company is a small or medium size business, it is possible they

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

may have to file bankruptcy to protect themselves from the financial liabilities occurring from the breach.

One high profile case where a company was required to comply with the new law was reported to the media in November 2003. This financial organization informed some of their customers that personal account information was stolen from an office in California. The types of information that were stolen included the customer's name, address, Social Security number and account numbers. These types of personal information are directly covered in the SB 1386. While the financial organization has not currently released to the media how many total customers were affected, they have stated it was a small number of their customers. The financial organization, according the NetworkWorldFusion article, has since taken the necessary steps to protect their customers against fraud. They have given each customer a new account; alerted the major credit reporting agencies of the incident, and even hired a company to help watch the accounts for any unusual activity on the customer's accounts (Niccolai). Based on the article, it appears that the financial organization is handling the incident within the guidelines of the SB 1386. It is important for other companies to consider the best ways to prevent this type of incident from even occurring, thus protecting one of the most important assets a company has; its reputation.

What consumers should do if notified of an information breach?

Individual and consumers need to be prepared and have an understanding of what to do if they receive a SB 1386 notice from an organization. One of the first recommendations would be not to panic. Just because you have received a notice, it does not mean that your personal data is being used fraudulently. However, it also does not mean you should toss the notice in the garbage and forget it. You should begin to review and monitor all your financial, bank, brokerage and credit statements for any unusual activities. Also, don't forget to monitor any employer based accounts like 401k or cash balance plans and stock plans as these could also be at risk. If you are not comfortable with just monitoring your accounts, you can cancel your bank debit and credit cards and receive new accounts. Contact all financial institutions that you do business with and let them know that you are to be contacted at a set phone number before any new cards, loans or large withdrawal are made on your accounts. If the breach occurred at your primary financial organization, you may need to determine if you still feel comfortable doing business with them. If not, cancel your accounts or business with them, but be sure that they know why you are withdrawing your business. This will send the message that mishandling of personal data will cost them your business and your money You may have not received a notice that your personal information may have been taken, but if you have reason to believe that your identity has been comprised, you should follow the same steps as above(StrongAuth, p.10-11).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SB 1386, which products or services can help?

As with any of the new laws that have come about in the recent years to combat the misuse of personal data, there are always numerous companies that are ready to jump on the bandwagon with their "quick" solutions. This is also the case with the passing of the SB 1386. Unfortunately, there are no simple solutions or a single product to protect your company's sensitive data. To adequately protect sensitive data, policies and procedure must be in place and enforced first before products can be used to supplement the protection of the data.

One of the types of products that I would propose to use for support of the SB 1386 requirements is a product that will protect the user's hard drive. This type of product provides the tools to encrypt each users PC hard drive using AES, an US government standard or RSA and Elliptic Curve Diffie-Hellman, both public-private key algorithms. This portion of this type of product will provide strong encryption on all users computer both desktops and laptops. After the product has been installed the user will be prompted to enter a password each time the PC is booted. With the correct password, the encryption/decryption engine is engaged and the PC operates as normal. However, if the password is wrong, then the product will lock out the user until they have entered the correct password (PCGuardian, p.1-2). This will prevent sensitive data from being retrieved if the computer is accessed improperly, stolen or lost. This type of product could have protected the heath care organization on December 14, 2002, when a thief stole laptops that contained the names, addresses, telephone numbers, birth dates and Social Security numbers of 562,000 military members and their dependents (Feinstein, p.1). The thief would have ended up with worthless hardware instead of valuable private information. All laptops that house sensitive information should have some type of product that will protect the information from being accessed by unauthorized persons.

There is also the vulnerability of sensitive data being transmitted via email. There are security products that provide an enterprise mail protection solution that are designed to provide email security with minimum disruption to the way the user sends their email. One such mail product uses an algorithm with a 256-bit encryption key which provides strong encryption and would minimize the risks of data being exposed to unauthorized personnel. This type product also allows encryption and decryption to take place "on-the-fly" without the use of key servers, certificate authorities or Public Key Infrastructure (PKI) which is resource intensive and costly. It is also easy and convenient for users that do not have the software to receive secure information from users that have the software. All the receiver would need to read or decrypt the message would be a password which the creator of the message could send by an out-of-band means (PCGuardian, p.1-2). While this type of product provides an excellent method to send and receive encrypted email messages, any product's success will depend on the user using the product when sending sensitive data.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Consumers also can opt to utilize services that many financial and insurance companies are currently offering their clients to protect against identity theft. These types of products can provide coverage for a fee, expenses caused by having to recovery a stolen identity, loss of wages as a result of having to be away from work to re-establish identity, legal defense costs, and other miscellaneous expenses, and most provide a customer hotline to assist the customer to understand the identity theft. There are companies offering "free" identity theft services, which provide limited services. The consumer should carefully review all services and coverage to ensure they receive the necessary and desired level of service to adequately protect themselves from identity theft.

Ways to ensure compliance

Companies are protecting the data on their database servers using varying types of encryption. Most database applications that are currently in use offer some form of proprietary encryption. While these types of encryption provide protection, they are not as strong or have not been tested extensively since most companies will not release their algorithms to the public for testing. If the database server is using a proprietary form of encryption, it may be questionable to rely on this as a safeharbor to the requirements of SB 1386 law.

Vendors are approaching support to the new law in other ways besides the obvious means of providing encryption for the data that needs protection. Vendors are providing packaged templates for SB 1386 and other current regulatory laws. These templates will assist companies that may not have information security or compliance departments from having to hire staff to develop roles and procedures for compliance with the new laws. Basically, they provide all the necessary training and policy information that is customizable for any size company within days instead of months or years. Many companies have hired the staffs that are qualified to develop and implement security programs to comply with existing and new legislation. Unfortunately, there are many companies that do not have the resources to comply with the new legislation and this can place financial hardships on these businesses.

Another method companies are using to protect themselves and limit their financial liabilities in response to SB 1386 and other recently passed legislation, is cyber-liability insurance. While your insurance agent may not be knocking on your door to sell your company this type of coverage; it is available and has been for quite sometime. In order to determine if the company would require this type of coverage, they should have their risk manager review the types of insurances available from the insurance broker and the costs for the coverage. After reviewing the findings based on the risks associated with the business, the risk manager would select the coverage that provides the best overall protection for the business. This process is very critical since each business could have a very different level of risk associated with the services or products that they provide. Businesses should also determine whether or not it has a regulatory requirement

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to carry additional insurance coverage's such as cyber-insurance to protect the privacy of individuals.

Companies that have a well established security programs and utilize standards such as ISO17799 can reduce the cost of cyber-insurance because of lower risk to their systems. Insurance companies may, however, request that an outside or third party risk assessment be performed on the organization to test the controls of the program. This will ensure that controls are functioning properly. If the organizations controls are deemed to mitigate risk, then they can and will be offered lower rates for cyber-insurance from the agent. While cyber-insurance is not appropriate or needed at every company, it definitely provides additional coverage for legal liabilities and loss or damage due to attacks to computer systems (Armstrong p.40-41).

The passage of SB 1386 should ensure that business and government entities take steps to protect personal and sensitive information from unauthorized breaches, either externally or internally. This bill is far reaching beyond the state of California businesses as it also affects any business that has customers in California. The enactment of SB 1386 will also lay the ground work for other states to enact their own laws after seeing the effects of SB 1386. There is the possibility of a federally mandated law being passed; Senator Diane Feinstein is actively supporting a bill that is patterned after the California law to address the privacy issue at the federal level but currently has no cosponsors and has received opposition the technology industry.

This new federal act, which is called the Notification of Risk to Personal Data Act, would define a national standard for consumers to receive notification of a database breach. It would allow the California law to remain in place but would preempt any state laws that conflicted, so that organizations would not have to try to comply with all the different states in which they may do business. This act would cover every U.S. business and government organization. This would send a clear message to all businesses and government agencies that they must comply and protect customer's information. There would be no chance for misinterpretation on whether the business was required to comply because they conducted business or had customers in an affected state. The penalties for not complying with the Notification of Risk to Personal Data Act could be as steep as $5,000 per occurrence or up to $25,000 per day the violation was allowed to continue (Threat Focus). Senator Feinstein summarized it best, "This bill has a tough but fair endorsement regime, and will give ordinary Americans more control and confidence about the safety of the personal information".

While these acts and new laws address customer information, what is not addressed is the overall security posture of an organization. If information was protected properly thorough out the organization from beginning to end, laws such as SB 1386 would not be necessary. For example, the new Corporate Information Security Accountability Act of 2003 requires a company to publish a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

notice proclaiming how well the company secures its Information Technology infrastructure and include it in their annual stockholders report (Rapoza). It would be available for all concerned parties to read. A savvy consumer may not want to risk doing business with a company that provided poor or minimal information security. This type of act could equate to a "scarlet letter" for a business that provided insufficient information security.

SB 1386 has a new name "Notice of Security Breach"

During the research for this paper, SB 1386 was enacted into law and is now known as the Notice of Security Breach – California Civil Code Sections 1798.29 and 1798.82 – 1798.84 (Office of Privacy Protection). While the name of the bill has changed, the bill itself remains the same. Companies should review their policies and standards to ensure they are updated accordingly to reflect the new name.

Conclusions

In summary, I believe this type of legislation is necessary to protect the privacy of information for all individuals. For those of us who have chosen a career ensuring companies are providing adequate information security, each new law passed or enacted also provides us a little more job security. Companies will continue to find it difficult to comply with the quickly passed and enacted laws and will require the services of competent information security personnel and consultants to reduce the risk of their legal and financial liabilities. Companies that choose to ignore the risks of the new laws and acts will surely, in some manner, be asked to pay a price they won't be able or willing to pay.

To ensure protection and reduce the risk of liabilities from the new law, I would recommend encrypting all data that is classified as non public information as per the individual company's standards or policies. This would include the information that was required by the new law and also include any information that the company consider "non public" information. This information may include data such as home phone, date of birth or family status. This solution complies with the Notice of Security Breach law as well as any data classification the company may have, however at an increased cost and system overhead.

One final closing remark; if companies' security awareness training was taken as serious as it should be, many breaches and misuse of information could be prevented. There is nothing more dangerous to an organization than an untrained employee. The old saying "an ounce of prevention is worth a pound of cure", never was more true than in the area of information protection. With greater awareness, there may be less need for legislation and consumers would be the winners.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

List of References

Armstrong, Illena. "A Risky Business Insurance in Cyberspace." SC Magazine. July 2003 (2003): 40-41.

Feinstein, Dianne. "Senator Feinstein Seeks to Ensure Individuals are Notified when Personal Information is Stolen from Databases." Home Page. 26 June 2003. URL: http://Feinstein.senate.gov/03Releases/datasecurityrelease.htm (24 Nov. 2003).

Hulme, George. "California Security Law Background." Information Week. June 23 2003 URL: www.informationweek.com/story/showArticle.jhtml?articleID=10700814&fb=20030l (3 July 2003).

Murray, Louise. "Breaches Forced into Public Domain." SC Magazine. July 2003 (2003): p.22.

Niccolai, James. "Wells Fargo Offers Reward for Stolen Computers." NetworkWorldFusion. URL:http://www.nwfusion.com/news/2003/1122wellsfargo.html (11 Nov. 2003).

Office of Privacy Protection. "Notice of Security Breach – Civil Code Sections 1798.29 and 1798.82 -1798.84." 24 June 2003. URL: http://www.privacy.ca.gov/code/cc1798.291798.82.htm (24 Nov. 2003)

PCGuardian Technologies. "Encryption Plus Email." Home Page. URL: http://www.pcguardiantechnologies.com/Encryption_Plus_Hard_Disk/index.html (28 July 2003).

PCGuardian Technologies. "Encryption Plus Hard Disk." Home Page. URL: http://www.pcguardiantechnologies.com/Encryption_Plus_Email/index.html (28 July 2003).

Peace, Steve. "SB 1386 Chaptered Bill Text." Home Page. 26 Sept. 2002. URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (10 July 2003).

Poulsen, Kevin. "California Disclosure Law has National Reach." SecurityFocus. 6 Jan. 2003. URL: http://www.securityfocus.com/news/1984 (8 Jan. 2004).

Rapoza, Jim. "Tech Direction Bill targets IT security." *EWEEK*. November 10 2003 (2003): 64.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Sabett, Randy. “State of Confusion.” Infosecurity. June 2003. URL: http://www.infosecuritymag.com/2003/jun/lawandregs.shtml (2 July 2003)

“StrongAuth SB 1386 Frequently Asked Questions 301” 6 Dec. 2002. StrongAuth, SB 1386 Resource Center URL: http://www.strongauth.com/sb1386/sb1386faq.html (22 July 2003).

Threat Focus. “Notification of Risk to Personal Data Act”. Threat Focus Security Compliance URL: http://www.threatfocus.com/norpda.php (24 Nov. 2003).

Vijayan, Jaikumar. “Will Firms Follow New California Privacy Law?”. PCWorld. 09 May 2003. URL: http://www.pcworld.com/news/article/0,aid,110678,00.asp (2 July 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.