Global Information Assurance Certification Paper

More than Secure Communications To Consider

GIAC Security Essentials Certification
Practical Assignment
Version 1.4b, Option 1
By: Ross Casanova
June 2, 2003

Table of Content

Abstract

This document provides a high-level analysis of proposed legislation *California State Senate Bill 1386 (SB 1386) - Draft Domestic Security Enhancement Act of 2003* and its possible implications on global business. With the evolution of e-commerce and identity theft booming, securing one's system has risen in priority. However, effective design and enforcement of identity theft protection measures has a long way to go, and with the proposal of new legislations to protect consumers, system owners now need to consider more than just the security of their communications and data.

Introduction

With the evolution of the Internet having reached far beyond its original conception of research, the number of government technology labs and communication centers and their security concerns for data confidentiality, integrity, availability, authentication, and non-repudiation has sky-rocketed. The Internet processes more then just bits of information; it processes bits of our lives. With so much personal information about individuals now being collected and maintained on computer systems, the security of these systems becomes paramount (see Federal Information Security Management Act of 2002 (FISMA).

The truth is, however, that few people truly understand computer security and it's implementation as advertised by computer-security companies that boast such features as hacker-proof software, Data Encryption Standard (DES), triple-DES, Advanced Encryption Standard (AES) and Secure Socket Layer (SSL).. SB 1386 addresses the issue of widespread reliance on these measures compounded by the need for protection of personal information. With today's hacker technologies, it is obvious that seemingly strong cryptography or supposedly unbreakable security is broken all the time. Additionally, as newspapers and security companies report security bugs and flaws, it becomes increasingly clear that effectiveness of security measures becomes relative to the time at which it is applied. The term "security," therefore, doesn't have much meaning unless you also know, "Secure from whom?" or "Secure for how long?"

Last April a hacker broke into computer systems at the Teale Data Center, which maintains personal information on 265,000 California state employees. In December 2002, TriWest Healthcare Alliance, which handles healthcare for 1.1 million members of the U.S. military, had computers stolen from its facility in Arizona that contained personal information (names, social security numbers, and medical claims history) of over 500,000 members of the military, some of whom are California residents. Recently, hackers broke into a University of Texas database and stole the names, social security numbers, and e-mail addresses of more than 55,000 students, former students, and employees (some of the victims were California residents attending the University of Texas).

These are just a few of the types of information stored on computer systems, and if this compromised information was intended or utilized for identity theft it would be one of the biggest cases in the country. All of these agencies and organizations mentioned could be impacted by SB 1386.

California Senate Bill 1386

California state legislators concerned with these types of attacks responded by passing Senate Bill 1386, which was signed by Governor Grey Davis on September 25, 2002 and which will take effect on July 1, 2003. The new law will ensure that all Californians receive prompt notification when a computer system owned by a state agency, person, or business is compromised and personal information (as defined in the Act) is exposed. (Information that is lawfully available to the general public from government records, however, is not considered confidential personal information.) The objective of such notification is to enable the affected individuals to take immediate steps to protect their identity. This bill may set precedence for other states once it has been successfully tested in a court of law. One concern, however, is that, without Federal regulation or intervention, states may only incorporate portions of SB 1386 in conjunction with other state-specific legislation, which could lead to a complicated weave of rules and regulations across the United States, thereby placing incredible restrictions on e-commerce and possibly global business.

In essence, SB 1386 amends the California Civil Code (Information Practices Act) by requiring immediate notification to California residents when their personal information has been compromised through a breach of system security (including University of California (UC) systems) and in cases where there is a "reasonable belief" that an unauthorized person has acquired their *unencrypted* personal (confidential) information.

The data covered by this law is an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver license number or California identification card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

In other words, once a hard drive at a data warehouse or an agency or business has been breached the system owner must notify California residents of the incident if it can be said with reasonable certainty that the information has been compromised. While this law accounts for systems and databases maintained by California state agencies, such as the Department of Motor Vehicles and local law enforcement agencies, as well as any person or business that conducts

business in California, it may also impact global businesses that may store California residents' information as a result of e-business.

Breach of Security

Under SB 1386, a breach is considered to be any ***unauthorized access*** of a computer and its data. So, if a business or agency has a policy authorizing access to its computers or data, any access outside the scope of that policy is considered unauthorized and must be reported if the system owner stores California residents' information.

Problem

To illustrate the potential impact that this bill may have, take, for example, a small Web-based business operating from a state other than California. To comply with the necessary security precautions from a hardware and software perspective, this business may need to invest several thousand dollars to upgrade their equipment or infrastructure to sufficiently track any potential intrusions. "If a small Web business with several thousand customers, some of whom reside in California, utilizes an outsourced 'managed hosting service' or ASP to host its infrastructure, databases, and website, will that business be liable for a breach of this law if the hosting service does not notify the company that its security has been breached?" This question, raised by the CEO of an online security company, demonstrates a concern that may impact global businesses and the need for Federal intervention in addressing cross-state communications.

Confusion

Another provision of this bill that could have a significant impact in security circles is in its explanation of encryption—or lack there of. The bill requires notification of California residents when there is a "reasonable belief" that an unauthorized person has acquired a resident's *unencrypted* personal (confidential) information. To quote from the original bill text, SB 1386 **will**…

> Require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

However, the bill fails to clarify what is meant by "unencrypted;" nor does it define encryption or identify if the data is to be encrypted in transit or at rest on the

server. For example, can someone use ROT13[1], which rotates the alphabet 13 places to encrypt data and argue that since they encrypted the data they would be exempt from the notification requirements of SB 1386?

Is ROT13 an encryption method?

To demonstrate the ROT13 encryption; the following is an example of a ROT13 script, which should work with all versions of UNIX "tr" (translate):

```
#! /bin/sh
tr 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'\
  'nopqrstuvwxyzabcdefghijklmNOPQRSTUVWXYZABCDEFGHIJKLM'
```

Even with better versions of "tr" which should allow this syntax we have encryption:

```
#! /bin/sh
tr 'a-zA-Z' 'n-za-mN-ZA-M'
```

This shows that ROT13, although weak and not practical in today's encryption environment, is technically an encryption method. Therefore, in terms of responsibility under SB 1386, what characteristics defines the type of encryption that would satisfy this bill's requirements and should organizations use Federal standards to define encryption or should states develop their own standards? This question has been raised throughout the security and Internet community, which is monitoring this legislation. However, the courts will most likely look to industry standards for guidance and select the specifications that they believe most accurately reflect standards that can withstand litigation—an activity that may raise more questions than it answers.

What is encryption

First, let's look at how encryption is usually defined:

The Domestic Security Enhancement Act defines encryption as "the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information."

[1] ROT13 is a simple Caesar-cipher encryption that replaces each English letter with the one 13 places forward or back along the alphabet. For example, "The butler did it!" becomes "Gur ohgyre qvq vg!"

One must keep in mind that, when selecting an encryption technique, understanding “risk” is a key factor in the decision. The question here is “what is the extent of risk?” and “how long will it endure?”

Techniques

Encryption techniques are used to protect against the risks associated with the transmission and storage of confidential or sensitive information, which would include the information identified in SB 1386 as personal (confidential) information. Data encryption is used in communications environments to protect against unauthorized or accidental access to information in that it prevents recipients of encrypted data from interpreting its meaning. Additionally, data encryption is used to detect the modification of transmitted data.

Types of cryptosystems

There are two kinds of cryptosystems: *symmetric* and *asymmetric*.

Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt. This type of cryptosystem has a problem, however: how do you transport the secret key from the sender to the recipient securely and in a tamperproof fashion? If you could send the secret key securely, then, in theory, you would not need the symmetric cryptosystem in the first place—you would simply use that secure channel to send your message or data. Frequently, trusted couriers are used as a solution to this problem.

Asymmetric cryptosystems (also called *public key* cryptosystems) use one key (the public key) to encrypt and a different key (the private key) to decrypt, such as RSA (an algorithm invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman).

Encryption and SB 1386

This bill fails to identify a requirement for any form of encryption. The language used in this bill also suggests that notification would be necessary if the unencrypted information “is reasonably believed to have been acquired” and not that the unencrypted information itself was transmitted. In other words, if the information that was stolen or “acquired by an unauthorized person” (even if encrypted) could be decrypted into plain text (either via a weak encryption scheme such as ROT13, or if there is evidence the encryption keys (*symmetric* and *asymmetric*) were compromised), would this information need to be reported? Do we then report all attempted or possible penetrations? What would the liability be?

Secondly, what if an agency or business does have an encrypted database? Despite the encryption, an "attacker" may be able to monitor the plaintext traffic over http from the front-end web server (which is fed data from the encrypted

database (DB)) to the remote browser client. Clearly, this situation is a breach, as well. In this case, the "attacker" does not get access to the entire database. Rather, he is able to view session specific plaintext packet dumps. If the breach occurred on the agency or business network, it is obvious that this would need to be disclosed per the bill. However, what if the breach occurred outside of their network and affected sessions between their network and provider Yankee Blue (a fictitious business for discussion purposes only)? Does the bill still require the business to disclose the compromise?

What if the data moves over the net via Secure Socket Layer (SSL), one of the most widely used encryption technologies for the Internet? SSL can encrypt information between computers. However, the technology has encryption starting and ending points. Attacks to computers can occur before and after these encryption points, causing a breach to the system. Therefore, an organization is obviously still liable to report a breach under SB 1386 even with SSL applied.

Additionally, even within SSL, there is a wide variety of implementations and key lengths. The encryption algorithm could just as well be ROT13. What if SSL is used to successfully move data over the net to a remote user's workstation where it is then stored unencrypted. If the user's system is compromised and the data is "acquired by an unauthorized person" (researcher), what actions are necessary based upon the requirements of SB 1386, and what are the originating organization's responsibilities?

Security vulnerabilities

If these examples are valid security concerns and if this bill may indeed impact global e-business, what if we now add the security companies that identify and exploit security holes in software or operating systems. A few years ago a security company discovered a dangerous security hole in a software company's Web server software. The security company, believing that the software manufacturer "was not giving the problem the attention it deserved," released not only a description of the hole, but two working demonstration programs that allowed anyone to break into an NT server. The break-in codes appeared to work on any server from which a Web page could be retrieved, even if a firewall was present. The security company explained its decision to disclose the bug, and to publish the programs that let anyone readily exploit it, in a brief note on its Website. Their Website noted:

"We are a full-disclosure security team…. If our team starts hiding the facts, we'll be no better than a software vendor that rushes insecure products to market."

This perspective raises an interesting point. On the one hand; the global community, especially agencies and businesses which rely on or use commercial off the shelf (COTS) software programs to protect their servers and data, needs to be made aware of any potential vulnerabilities software they run on their

systems may pose to their information, particularly if they are storing or processing information which falls under the provision of SB 1386. On the other hand, who is liable if a business or agency's data is compromised due to a security hole that a security company has made public and for which it has published a program enabling anyone to readily exploit that hole? What are the implications of SB 1386?

In its defense, the security company announced the security hole and released a "hacking program," stating that a moderately skilled hacker, armed with the knowledge that the bug existed, could easily craft a program to exploit it in less than two hours. This may have been true for skilled hackers, but through this hacking program, unskilled hackers—or script kiddies—would also be able to attack random sites, and therefore escalate the problem, before the software company released a workable patch that the global businesses affected by the weakness could have employed to fix the hole.

Reporting and SB 1386

All of this brings us to the reporting dilemma.

The law generally requires people to act "reasonably." That is, a vendor must exercise due care to the community of people who use or rely upon its product and makes certain warranties and representations about the product itself.

Similarly, a person discovering a vulnerability is required to act "reasonably." For example, publicly reporting a fictitious vulnerability would most likely subject the reporter to liability for tortious interference with business relationships, business defamation, or other potential liability. Should the same hold true for reporting an actual vulnerability if accompanied by the code which can enable others to exploit the vulnerability? This is a matter of opinion as discovered from online sampling and chat room results.

It is clear that a standard needs to be developed for reporting, which should take into consideration the consequences of bills like SB 1386. This topic, while outside the scope of this paper, is definitely one that needs to be studied in further detail.

Preparation for SB 1386

Companies or agencies must begin to consider the impact this bill may have on their businesses despite their being in compliance with its intent. In addition to their continuity of operations (COOP) or disaster recovery plans (DRP), they now need to incorporate a plan for SB 1386 compliance. The law requires that California residents whose information has been compromised must be notified in the most expedient manner possible and without unreasonable delay. Although various options are available to accomplish this, such as direct mail, an electronic notice that conforms to Federal standards, or by substitute notice (i.e.,

e-mail, posting on a publicly-accessible website that the business or agency maintains, or notification to major statewide media such as newspapers, TV and radio). However, depending on an organization's customer base, notification can become costly. System owners must therefore take these costs into account just as they would factor in their COOP or DRP costs. Every agency or business to which this law applies must determine for itself what this potential cost will be and further determine what it is willing to spend to mitigate the risks of noncompliance with the bill (i.e. lawsuits and damages due to a breach, cost of notification, etc).

A business or agency can also mitigate these costs by implementing preventive measures, which can involve:

- Implementing and documenting rigorous policies and controls;
- Re-architecting the critical infrastructure and /or applications; and
- Using encryption for data storage and transmission.

While risk cannot be eliminated completely without impacting the business process significantly, preventive measures can help in keeping the risk to manageable level.

Conclusion

With the Presidents policy for fostering e-commerce in full swing, California legislators are looking out for its' residents by enacting SB 1386. Though the bill is well intentioned to protect the citizens' private information, it has many flaws and weaknesses as evidenced by a technical ambiguity, lack of reporting structure, and difficulty of enforcement when integrated with other laws governing business operations outside its jurisdiction. While the intent of this new law is to protect consumers from identity theft by providing them with notification when their personal information has possibly been compromised, the bill does very little to directly protect against identity theft. Usually, only "Criminal Statutes" deter thieves. This statute might make it more difficult for hackers to obtain their objectives if businesses follow the bill's implied message: get security and encryption. Nevertheless, the bill itself won't deter hackers. Additionally, one of the big open issues relates to the portions of the law that deal with encryption. However, even with these encryption issues, other states will likely follow California's lead as they, too, seek to protect individuals from identity theft (although their particular actions may depend on how an actual case is tried in court were an agency or business ever prosecuted for an SB 1386 violation). While we can attempt to protect our citizens from these types of crimes through the creation of identity theft laws, today's electronic environment makes it practically impossible to implement and enforce these new laws. Identity theft continues to increase, while prosecution rates for identity-theft crimes remains flat. For now, the best individuals can do is attempt to minimize the damage after the fact and hope that companies and agencies implement stronger

authentication to protect your data. Although there are technical solutions that companies or agencies can employ to solve this type of problem, as with any complex problem that hasn't received attention for many years, getting started on the effort is the most difficult issue.

Bibliography

David J. McIntyre, Jr., President and CEO, TriWest Healthcare Alliance, "Important communication concerning identification theft" December 31, 2002
URL: http://www.triwest.com/announcement/press_release.asp
http://www.triwest.com/announcement/

Associated Press, "Hugh military ID theft; reward offered" January 1, 2003
URL:
http://www.cnn.com/2003/TECH/biztech/01/01/pentagon.computerthef.ap/index.html

Senator Peace, "Senate Bill No. 1386", California, February 12, 2002
URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Jacqueline Craig, "Identity theft: New California law will impact campus departments," April 16, URL: http://istpub.berkeley.edu:4201/bcc/Spring2003/news.sb1386.html

Thawte, "Criminalizing crypto a bad idea" March 2003
URL: http://www.thawte.com/html/CORPORATE/news/crimaliseEnc.html

Mark Rasch, "The Consequences of Criminalizing Crypto," March 3, 2003
URL: http://www.securityfocus.com/columnists/145

Kevin Poulsen, "Ashcroft proposes vast new surveillance powers," February 7, 2003
URL: http://www.securityfocus.com/news/2296

Erik Laykin, "New California Law to Impact Global Business - SB 1386", May 27, 2003
URL: http://www.onlinesecurity.com/index.php

Rot13.com, This link provides an example of rot13 cipher
URL: http://www.rot13.com/

Question from Bernie "Full Disclosure: Re: California State Bill SB 1386," April 2, 2003
URL: http://lists.insecure.org/lists/fulldisclosure/2003/Apr/0046.html

"Domestic Security Enhancement Act of 2003", Draft – January 9, 2003
URL: http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf

Bureau of Industry and Security, Department of Commerce
URL: http://www.bxa.doc.gov/Encryption/Default.htm

Dan Froomkin "Deciphering Encryption", May 8, 1998
URL: http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm

U.S. Department of Homeland Security, Federal Computer Incident Response Center
http://www.fedcirc.gov/library/legislation/FISMA.html