Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Case Study: One Companys Response to the California Identity Theft Law

This case study tells the story of how our company dealt with two challenges: suffering the theft of some confidential client data; and, bringing our systems into compliance with the new California identity theft law, SB 1386 that set compliance-goals to protect consumers. An inventory and assessment of over 100 application environments categorized the risk factors emanating from various tiers: Back-end servers, middle-tier (including network) systems, client-tier systems and business-risk. Risks were methodically iden...

Copyright SANS Institute

Author Retains Full Rights

AD

Case Study: One Company's Response to the California Identity Theft Law

SANS Security Essentials
GSEC Practical Assignment, Version 1.4b
Option 2—Case Study in Information Security

Gordon Bass

September 15, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

The California identity theft law, SB 1386, went into effect July 1, 2003, soon after several cases of identity theft were perpetrated by individuals who had stolen our clients' confidential data. The convergence of these events set the stage for risk-mitigation and remediation efforts by the CISO's office, for which I was the assigned lead in my new role of Deputy CISO. This case study tells the story of how our company dealt with these twin challenges, of suffering the theft of some confidential client data, at the same time a new law was enacted that set compliance-goals to protect consumers.

An inventory and assessment of over 100 application environments categorized the risk factors emanating from various tiers: Back-end servers, middle-tier (including network) systems, client-tier systems and business-risk. Risks were methodically identified in this fashion and vetted by stakeholders, along with proposed mitigation and remediation actions. Next, the highest-risk vulnerabilities were identified and fixed first. At the same time, an education program was begun, with help from our general counsel, to educate staff and vendors on enhanced guidelines for handling confidential client data. The results of our efforts have created a more secure environment that better protects our clients' confidential information. We also have an enhanced corporate-wide understanding of, and commitment to, these new guidelines that will serve us well, as we remediate the remaining existing systems and deploy new systems in the future.

Before: "Sure, identity theft is a problem and we're *already* doing our part to combat it."

Do you think your company's traditional identity-theft countermeasures are adequate? Guess again. As with criminals conducting exploits in every other area of information security, the perpetrators of identity theft just keep getting smarter and cleverer, and striking more frequently. So our defenses have to continuously improve as well, to keep up. Defenses that may once have been adequate are no longer so. Identity theft is not a new problem; it's a problem that has probably been around since the dawn of civilization, but lately, it just seems to keep getting bigger and bigger. According to the accepted formula of *Risk = Vulnerability X Threat*, we can see that the dramatic increase in the incidence of identity theft directly translates into an increased Threat factor and consequently into bigger risks for most companies to manage. These new realities hit home for me during the past six months, as my company struggled to recover from a case of identity theft and plan to comply with a new California law.

Sizing up the Problem

The magnitude of the problem, generally, is that 7-10 million Americans were victimized by identity theft last year. The typical victim lost $800 and will spend two years clearing his name. Aggregate annual cost to businesses and consumers approached $53 billion. (CU, p. 12, McGuire)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This problem has attracted major industry attention. Look at the heavyweights that announced this month that they are founding a coalition to fight identity theft: Amazon.com, Business Software Alliance, Cyveillance, Inc., eBay, Information Technology Association of America, McAfee Security, Microsoft, RSA Security Inc., TechNet, Verisign, Visa U.S.A., WholeSecurity, Inc., and Zone Labs, Inc. (ITAA)

Problems in California

In California, a break-in occurred April 5, 2002, into a database at the state's Stephen P. Teale Data Center, resulting in unauthorized access to the computer records of all 265,000 state government employees, including that of Gov. Gray Davis. The incident was discovered by the state controller's office May 7, and disclosed to the public May 24. The handling of the incident provoked the California Union of Safety Employees, which criticized state controller Kathleen Connell for the delay in informing victims that their personal information may have been compromised. (Vijayan)

This breach in security came at a time when California legislators had already enacted several anti-identity-theft laws. Angered over this theft of state employee data, legislators enacted yet another new California law, known as SB 1386 and introduced by Senator Steve Peace. It states:

> This bill, operative July 1, 2003, would 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. (Peace)

This personal information is defined within SB 1386 as SSN (Social Security number), driver's license number, state-issued ID card number, or bank account numbers and access codes. The logic behind this law is to force companies to either encrypt citizens' private information, making it useless if stolen, or make prompt disclosure in the event of theft. Therefore, companies that proactively protect the confidentiality of their clients' data via encryption do not need to do anything further in the event of a breach in the security of that data. Companies that *do not* encrypt data must, in the event of a breach, promptly react by notifying the owners of the data whose data was compromised. Such notification is considered to be worthwhile to the consumer whose private information may have been compromised, because then the consumer has time to take protective measures, such as inserting fraud-alerts in credit bureaus' records and even more drastic steps, such as closing existing accounts and opening new accounts. Most often, consumers are not aware their private information has been compromised until some later point when they discover they have already become victims. The legislature felt this law was necessary, because there have been many instances of companies not notifying consumers of breaches of the security of their private information; companies avoid disclosure because they fear the adverse publicity. Note that this law applies as well to companies and databases not located in California, so long as the compromised data belongs to California residents.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ID Theft Strikes Home

Meanwhile, our company had an incident of identity theft in the spring of 2003. There were 20+ clients whose identities were stolen and who had since learned that unauthorized purchases were made in their names. An employee apparently provided clients' SSNs and other personal data to identity thieves. Our company mailed letters to approximately 1300 clients who were determined to have been at risk. In the letters, a company executive advised clients of the situation and provided information about actions they should take to head off identity theft, including the need to contact the three major credit bureaus. The executive also committed the company to reimbursing clients for any costs they might incur in contacting the three credit bureaus. Last, but not least, the letter also shared details of the company's renewed commitment to data security and promised clients that they could rely on the company's extra attention to safeguarding their data in the future. A source familiar with the probe said an employee was suspected of providing clients' personal information—SSNs and other identifying data—to outsiders who then used the information to acquire credit cards and make purchases under the clients' names.

This was a perfect example of why one cannot rely only on perimeter defenses. I am happy to say, this was also a perfect example of a company voluntarily responding with full disclosure, in a responsible manner like that set forth by the new California law, even though the theft did not affect California residents and the law had not yet taken effect.

Stolen Laptops

Shortly before this, a new CRM system had been rolled out, utilizing laptops and WiFi technology at offsite client events. Unfortunately, some of these laptops, which could contain client SSNs, were stolen. Also most unfortunately, the data on these laptops were not encrypted, as our CISO had directed they should be, two years prior to the theft. Yes, there is an element of "I told you so!" in this recounting. We were lucky, though. Our assessment of what data had actually been stolen led us to conclude that no confidential client information had been compromised and therefore no client notifications were necessary, as we had done after the previous incident of identity theft. But, if we'd been unlucky, the stolen laptops could just as easily have contained confidential client information.

Insufficient Defenses

Let's summarize our "before" security posture and some of its consequences. With regard to risk, we had defenses in place for many traditional vulnerabilities. We had a good network security perimeter in place that, for the most part, was effectively keeping the bad guys out. An insider, for whom our good network security perimeter presented no obstacle, perpetrated identity theft; she was able to take advantage of a lax area of physical security and remove a sensitive paper document from company premises. Our CISO had calculated the risk in deploying unencrypted portable wireless CRM systems and, unfortunately, his directives to mitigate the risk were not followed. These systems operated outside our firewall and physical security perimeter; what security measures

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

were employed, we learned from experience, were inadequate. Defense in depth was not practiced, as it should have been. The consequence was loss of confidentiality or, more specifically, identity theft. Fortunately, data integrity and availability were not threatened, but our affected clients had little appreciation for that fact.

During: "We need to do more, *now*."

The convergence in time of these security incidents and the emergence of the new California legislation motivated us to concertedly pursue three courses of action, two of which I was made personally responsible for by our CISO.

Doing More, Part 1—Laptop Data Encryption

Our CISO pursued our first course of action. He determined that he would now force the issue of encryption of data on the CRM laptops. As one might guess, this time around he received complete concurrence to proceed from all IT and business stakeholders. Research was done on various alternative solutions that would achieve the goal of encrypting the data on the laptops. Encryption solutions could be employed at the Windows file system level and there were also database encryption methods that could be applied to the whole database or just selected data fields. After weighing the pros and cons of the alternatives from cost-effectiveness and time-to-deploy standpoints, the decision was made to employ the native Windows EFS (Encryption File System) on selected folders on every laptop. An added benefit of this approach was that EFS was transparent to the CRM application. Considering that this system encompassed over 3000 laptops, this was not a trivial matter.

A project manager was assigned responsibility for this new project and plans were developed that would complete encryption of specified folders on all 3000 laptops by July 1, the effective date for the new California law. Although the company had already demonstrated an interest in upholding the spirit of the California law, based on the prior instance of identity theft, the July 1 implementation date for the new law became a very symbolic stretch-goal to attain. On June 29, the implementation of EFS was completed. While this was an achievement that we could feel good about, the good feelings were tempered by the realization that it would have been far better and far easier to have incorporated security requirements into the original product design two years previously. At this point, our CISO also ordered an independent WiFi audit of this system's operating environment and we were able to confirm that the risk of "useful" data interception was extremely low due the frequency-hopping encrypted communications protocol employed.

Doing More, Part 2—Understanding the New Law

Our second course of action that I began pursuing was to gain an understanding of what the new California law really required, in terms of compliance. My interest was

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

much more than academic: In addition to the laptop-based CRM systems, we had potentially a hundred other applications that also used private identifiers, as defined by SB1386, that would require assessment and possibly risk-mitigation efforts. For example, the law speaks of *encryption* but does not specify *strength*. Is weak encryption acceptable? Our decision was to employ strong encryption, but this question presented an interesting potential loophole in the law that unscrupulous companies might take advantage of. We also began discussions with our general counsel in order to coordinate understanding and compliance activities related to the new law. Although our company had already demonstrated a commitment to adhering to the spirit of the new law, we needed to understand exactly what was required for compliance, in order to understand what contingency plans would be required to successfully and legally respond to any potential breach of security of data belonging to residents of California. Our company has a large presence in California and also conducts business with California residents from other locations and on various computer systems throughout the nation. In all these cases, this law applies equally, I found, unless one wants to get into constitutional debates over the sovereignty of states' laws. It is cheaper and easier to comply and, in any case, it is the right thing to do.

What are Other Companies Doing?

At one point during these discussions, it occurred to me that other companies must be struggling with some of these issues and it could be instructive to learn from their experiences. So I spent an afternoon conducting an Internet search to find out how other companies had implemented SB 1386 and, in particular, how they may have decided what encryption strategies, methods and tools to employ. I found many references to SB 1386 but I found absolutely nothing about how other companies were changing their systems to comply with the law. Could I be the only IT professional interested in SB 1386 compliance and contingency planning? This alludes to an interesting question: What must a company do to comply, anyway? There are two possible answers: 1) Encrypt private information so that in the event of theft, the company will not need to send disclosure notices to the citizens whose information was stolen; or 2) Comply with the disclosure specifications of the law, in the event of the theft of *unencrypted* private information. Option 1 is our preferred answer, because we do not want to endure the negative publicity that accompanies disclosure of the theft or loss of private client information. I concluded that most companies must be pursuing the "hope for the best" Option 2, since I had found no references to other companies that were implementing new encryption solutions.

There are other areas of SB 1386 that appear ambiguous, which I won't go into further at this point. Our general counsel offered to identify a California law firm that would consult with us on these issues. We did that, but my opinion was that this was not particularly helpful, since any clarifications needed to come from the California legislature or a California court, not from yet another law firm.

Federal Legislation Too?

During this timeframe, while I was researching SB 1386 compliance strategies, potential Federal legislation appeared that could adopt and simplify the principles of SB 1386.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Senator Dianne Feinstein (D-Calif.) jumped on the California bandwagon, introducing Federal legislation in June, 2003, modeled on the California law. This *"Notification of Risk to Personal Data Act"* would, in part, levy fines of up to $5000 per violation or $25,000 per day, to entities that don't comply with these notification guidelines. The legislation could also identify a clear national standard for protection and disclosure. (Feinstein)

Third-party Compliance

Another aspect of compliance that we contemplated was the need for us to sensitize third-party vendors, such as collocation data centers in which we housed client information, to our need for timely communication. In the event that one of our vendors experienced a security breach, I wanted to be sure that we would receive prompt notification from that vendor. This would be an essential component in our SB 1386 compliance program, since SB 1386 in turn requires prompt communication to consumers. I drafted a standard form letter which I asked vendors to print on their company letterhead and sign. The text is as follows:

> In the event of a breach of the security of a Company system hosted by Vendor (where "breach" means computerized data was, or is reasonably believed to have been, acquired by an unauthorized person), notification shall be made immediately following discovery, via phone call, email and letter, to both Vendor's regular Company POC and the Company's Chief Information Security Officer. In the notification, please identify pertinent details, including observed facts, suspected damage or loss, date & time of event, server(s) affected and database(s) affected.

Failures at Microsoft and Eli Lily

While conducting my research on SB 1386, I came across some very instructive material that illustrates the importance of compliance with privacy laws. There is a strict new government standard of performance that the Federal Trade Commission says companies must follow:

> It is not enough to make promises about protecting personal information, and then just hope that nothing bad happens or, if it does, that nobody finds out. Fulfilling privacy and security promises requires affirmative steps to ensure that personal information is appropriately protected from identity theft and other risks to consumers' personal information. (FTC)

If anyone doubts the seriousness of this statement by FTC Director J. Howard Beales, then consider what happened to Microsoft and Eli Lily: In 2002, the FTC brought enforcement actions against these companies for misrepresenting to consumers, the levels of security measures in place to protect the information collected from customers. According to Director Beales, the new standards of performance we must follow are: "(1) implement procedures needed to prevent or detect unauthorized access; (2) monitor the system for potential vulnerabilities; and (3) perform appropriate security audits or investigations." (FTC)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Doing More, Part 3—Identifying and Mitigating Risks

By now, we had made some significant progress over a period of a few short weeks. We had learned where we had some problem areas. We were now convinced we needed to do more to protect our confidential information. We had expeditiously encrypted data on 3000+ laptops. We had learned that the new California law was a two-edged sword: On the one hand it mandated a high level of compliance; on the other, it gave us ammunition to goad the rest of IT and the business units into better security practices. My research had reinforced the fact that our representations to clients that we would safeguard their data had better be accompanied by action, taking all prudent and reasonable measures. This sequence of events logically led to my next endeavor.

Our third major course of action that I pursued was to conduct an exhaustive "risk inventory" of every production system that might contain private client information. I created a Personal Identifier Survey form and gave copies to each of the three IT development groups. The survey asked respondents to identify and return to me within two weeks, the following information for each application system containing personal identifiers, for which the group was responsible:

1. Application name.
2. What personal identifiers exist? (SSN, driver's license number, state-issued ID card number, or account, credit card or debit card number and security code.)
3. Are any of these personal identifiers used as database keys? (This question was asked because I was interested in finding out how critical the personal identifiers were to the database design and whether they could potentially be encrypted.)
4. Are any of these personal identifiers encrypted or obfuscated? (This question was asked so we could identify applications that might already exercise the desired level of encryption of data. We also considered that obfuscation could be an effective alternative to encryption. For example, storing only the last four digits of a client's SSN would constitute obfuscation and would generally be considered an effective alternative to encryption.)
5. To who do these personal identifiers belong? (I wanted to find out whether the private identifiers belonged to clients, employees or affiliates, in order to better understand potential threats and risks.)
6. Where do these personal identifiers exist? Where are the databases and/or extract files and/or output files that contain personal identifiers? (The purpose of this question was to identify whether the data "lived" only in our physically secure data center or in other less-secure environments as well.)
7. Are these personal identifiers transmitted in the regular course of business? If so, how? (This question was to identify if data was transmitted via FTP or magnetic/optical media and, if so, was it encrypted or clear text.)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

8. How vulnerable is this information to theft or loss? Please consider internal, as well as external, threats. Respondents were asked to identify if potential threats were high, medium or low, in their opinion, and to provide an explanation of each. (The purpose of this very useful question was to motivate each respondent to think about her area of responsibility and what insight she could share about potential vulnerabilities and threats. Many of our follow-up action items originated with the answers to this question.)
9. Are there any risk-mitigation strategies you would recommend we adopt with regard to the safekeeping of the personal identifiers used in this application? (We also received quite a bit of useful insight in response to this question.)

In all, 40 applications were identified that contained clients' private information. My next step was to meet with application development and project management staff, to review the survey results and to evaluate our risks and possible mitigation strategies. As I proceeded with this task, I also began to create a document that contained our risk assessment summaries for each application.

Risk Assessment

Risk components assessed for each application included the following four categories: Backend, Middle-tier, Client-tier and Business risk. Each category of risk for each application was assigned a risk assessment of Low, Medium, High or Unknown, based on the best information we had available. Our intent was to discuss and validate these assessments with the responsible IT development groups by distributing the document for their review and follow up. The development groups were asked to review these assessments internally as well as with the end-user business units that owned the applications.

Risk categorization consisted of:

- Backend risk: Pertains to the security of the backend database server, or server upon which the source database resides in an n-tier architecture.
- Middle-tier risk: Pertains to the security of middle-tier application servers, security of network data communications and security of ancillary 3rd-party data processing.
- Client-tier risk: Pertains to what the end-user is capable of viewing, printing, extracting or downloading onto desktop and laptop workstations.
- Business risk: Pertains to business-process risk that was observed or may exist. For IT, this may be *informational* rather than *actionable* in nature, because it extends beyond the responsibility and authority of IT staff. Examples of this are end-user training on handling sensitive data and documents, securing unattended workstations, periodic audits to ensure end-user compliance and other functions under the supervision of business-unit management. Each business unit owner for each of these systems needs to conduct their own risk-assessment of these areas. Since in many cases we know less about the business risk, compared to the IT risk, the assessments

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

we assigned needed to be corroborated by the end-user business unit management and changed if necessary. Each development group was to review this information with their business-unit customers

Action Items

For each of the 40 applications, we identified recommended follow up action items for IT and for the business units:

- IT follow-up: This identified the recommended IT follow up actions. In addition to application-specific follow-up items that were identified elsewhere, these general follow-up items needed to be acted on for every application:
    - IT needs to research and offer appropriate encryption solutions for PI (personal information) data. Such solutions will afford encryption of PI data in the databases.
    - PI data used in development and test environments should be obfuscated; otherwise, it must be subject to the same precautions as the production data.
    - Every application should be checked to identify what PI data is extracted and copied to the client PC. Is this PI data necessary? Is it encrypted? Is it controlled in a secure manner? Is it removed when it is no longer needed?
    - Are SSNs and other PI data really necessary? Can other means of identification be used instead?
    - Review each application with the end-user business-owner, to best identify and mitigate risk.
- Business follow-up: This identified the recommended business-owner follow up actions. We needed the business owners of these applications to perform their own due-diligence to insure that data were being securely handled by their staff. In addition to application-specific follow-up items that were identified elsewhere, these general follow-up items needed to be acted on for every application:
    - Are business unit staff trained on handling sensitive data and documents, and securing unattended workstations?
    - Are business unit staff allowed to access sensitive personal information on screens and reports, only on a "need-to-know" basis?
    - Are business unit staff periodically audited by business-unit management to ensure compliance with these procedures?
    - Are business unit staff encrypting PI data that they transport on laptops, to afford some protection in the event of the loss or theft of the laptop?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Are SSNs and other PI data really necessary? Can other means of identification be used instead?

Our software development groups received and began reviewing this report. During the first week, I was pleased to find that development managers jumped on 5 of the 40 application risks in my report. Considering all the competing priorities these folks generally have to deal with, I was impressed to receive such a positive response this soon. Some of these risk issues were pretty serious, too. For example, we discovered that data, including SSNs, were extracted from a database and sent to a vendor that performed some outsourced processing. However, the vendor had no need for SSNs; why were these data even transmitted?! Some fixes like that were simple to make and easily reduced risk in demonstrable ways.

Quit Using SSNs

During this period of time, I awoke with a start one morning; I was hit with the sudden realization that we needed to stop using SSNs in our application databases. Instead, as a means of identification, we could rely on internally generated client ID numbers. The research I'd done on the Internet had suggested this approach. I began proposing to our software development groups that we pursue this strategy and I found nearly everyone receptive. In fact, our manager responsible for the payroll systems, immediately suggested ways he could cut back on the use of SSNs. Keep in mind, this came from possibly the only development group with a legitimate need to use SSNs! His first suggestion: Stop printing SSNs and bank account numbers on payroll remittance stubs. That change was easily made this month.

A few weeks later, our general counsel published a company guide to the use of confidential information. To my pleasant surprise, I found within a section that read:

> <u>Special Information on the use of Social Security Numbers</u>
>
> The company must refrain from using social security numbers as an identifier for any Subject or company employee unless such use is a legal necessity or required for administrative coordination, such as employment or payroll purposes. Company business units should use a system of alternative numbering. (Guidelines, p. 9)

This was great news. The CISO office and the general counsel's office were completely united on this issue; this would help in our efforts to educate our staff. I began to notice a groundswell of similar sentiment in the mass media as well:

> Identity theft is a problem largely because financial institutions, merchants, credit bureaus, and the government do not adequately safeguard vast databases and other records containing consumers' sensitive information, making it relatively easy for thieves—often insiders—to access these data. Many institutions use SSNs when other identifiers would suffice, fail to notify consumers when security breaches occur, and provide little help or recourse for consumers stuck cleaning up the mess. (CU, p.12-13)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Many of our software applications, unfortunately, make extensive use of SSNs and will need to be modified in later releases, or retired, to discontinue use of SSNs, even assuming we are able to get concurrence from the business owners. Therefore, other mitigation strategies have also been pursued. For example, a data warehousing application that provided 60 users with access to SSNs was modified so that only those users with a need-to-know, about 10 staff, could view the SSNs.

Positive Effects

We began to notice that the cumulative impact of these efforts was very positive. Many small improvements in security added up to a big overall impact. Not the least of these was the impact on our staff's mindsets. Throughout these months, we were all becoming more sensitized to the issue of heading off identity theft by limiting use of private identifiers and, when they must be used, enhancing the security employed. An example of this was a demonstration that I attended, in which a prototype of a new user account provisioning system was shown. I immediately noticed that SSN was used as an employee identifier in the system. After a short discussion with the lead architect, he readily agreed to remove SSN from the provisioning system.

After: "Identity theft *is* a big problem and We *are* doing more to fight it."

As of this time, we have successfully responded to instances of identity-theft by developing a process for risk-assessment and mitigation. We also have successfully mitigated 5 of the 40 identified applications that were determined to have been at risk. The remaining risks are methodically being prioritized and addressed through a variety of means by IT and the business owners. Company-wide, I observe that employees generally are more aware of the need to protect our clients' confidential information.

Recipe for Success

In retrospect, these are the steps we followed to achieve our current success.

- Identify the problem and the root cause. We had inadequate security for laptops and clients' personal information, based on the fact that thefts had occurred.
- Contain damage resulting from incidents. In the case of the thefts, we acted quickly to contain the damage to clients by notifying them.
- Apply lessons learned; prepare for future exploits by improving defenses. We learned that we needed to encrypt confidential information on laptops, as well as in other areas. We needed to better control paper documents containing personal information.
- Understand the requirements for change, the risk-mitigation and legal compliance goals. We learned as much as possible about the new California law and what we should do in order to be compliant.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Conduct a central inventory of known risks and categorize them as action items for IT or business units. This gave us a dashboard view of the risk mitigation tasks and our progress in executing those tasks.
- Validate the effectiveness of mitigation plans via inspection, test or analysis. Each risk-mitigation plan proposed needed to be vetted by the development group and the business owner in order to make sure we understood the problem and had identified the most cost-effective solution.
- Eliminate the use of personal identifiers, particularly SSNs, as much as possible. I realized that elimination of the use of SSNs, if viable, was the easiest and most effective method to reduce the risk of theft, thereof.
- Execute mitigation plans with a sense of purpose and urgency. Once high risks were identified, we began planning to mitigate them as quickly as possible. When I had momentum going with the team, it was best to keep plowing straight ahead so as to accomplish as many security improvements as possible while I had staffs' attention.
- Ask third-party vendors and contractors for written commitments to provide notification of any security breach at their facility. This was worthwhile because it set vendors' expectations and had a beneficial sensitizing effect.
- Apply "defense-in-depth." Nearly every one of our security defenses was vulnerable to failure or some exploit at one point or another. Creating concentric layers of defense provides desirable redundancy.
- Make use of SANS resources. "Section II, Defense in-Depth" was particularly helpful to me, providing many good ideas. It was a good source of best-practices talking points, which I used in discussions with other IT staff.

More Resources Needed

As I worked on these issues, I realized there are some resources that would be nice to have, if only they were available:

- The FTC web site is replete with information for consumers. It also advertises an upcoming "Business Information: Curbing Identity Theft" section of their website, which is not yet available. It would be very helpful to have FTC guidance and insights on how *businesses* can better protect data and comply with applicable Federal laws.
- It will be good to have clarification of the new California law, SB1386, and practical implementation guidelines to achieve compliance. Hopefully, this case study on the subject will be helpful in that regard.

Ongoing Efforts

What are our next steps? Well, after the remainder of our 40 application risks are mitigated, we will breathe easier, but not for long, since the work of securing the enterprise is never truly done. The challenge of combating identity-theft continues with

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

renewed vigor at this company. Currently we are feeling successful. My goal is to continue working diligently to keep things that way.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Consumers Union. "Identity Theft: 33 Million Victims and Counting." Consumer Reports. 68.10 (2003): 12-17.

Federal Trade Commission. "Prepared Statement of the Federal Trade Commission on Identity Theft." 3 Apr. 2003. URL: http://www.ftc.gov/opa/2003/04/idttestimony.htm (8 Sept. 2003).

Feinstein, Dianne. "Senator Feinstein Seeks to Ensure Individuals are Notified when Personal Information is Stolen from Databases." 26 June 2003. URL: http://www.senate.gov/~feinstein/03Releases/datasecurityrelease.htm (8 Sept. 2003)

"Guidelines for the Access, Use, Maintenance, and Disclosure of Confidential Information." July 2003 (2003): 9.

Information Technology Association of America. "Coalition Forming to Crack Down on Online Identity Theft." 2 Sept. 2003. URL: http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1062528130 (8 Sept. 2003).

McGuire, David. "FTC, Businesses Renew Fight Against ID Theft." washingtonpost.com. 3 Sept. 2003. URL: http://www.washingtonpost.com/wp-dyn/articles/A18833-2003Sep3.html (8 Sept. 2003).

Peace, Steve. "SB 1386." 12 Feb. 2002. URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (8 Sept. 2003).

Schwartz, Mathew. "California Privacy Law: Goodbye Good Intentions." Enterprise Systems. 23 July 2003. URL: http://www.esj.com/news/article.asp?EditorialsID=633 (8 Sept. 2003)

Thibodeau, Patrick. "California Leads Way on ID Theft Legislation." Computerworld. 13 Dec. 2002. URL: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,76721,00.html (8 Sept. 2003)

Vijayan, Jaikumar. "Recent Breaches Raise Specter of Liability Risks." Computerworld. 31 May 2002. URL: http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,71609,00.html (8 Sept. 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced