Global Information Assurance Certification Paper

Lou Mancel
November 11, 2003

Case Study: Securing a Windows environment against California SB 1386 using BindView bv-Control for Windows

GIAC Security Essentials Certification (GSEC)1.4b (August 2002)

Abstract

Our company is a security software development corporation that constantly is updating the queries in our vulnerability management tools. With new regulations coming out at a rapid pace, I needed to be able to provide a unique and valid set of queries to report against security breaches that are applicable to California SB 1386.

This study details key aspects of the project including:

Research of the California SB 1386
An overview of what was needed to be able to report my windows environment
Creation and testing of the queries needed
Submission of the results to Marketing

1. Problem Definition

In early July 2003, I was doing diligence by keeping up on the latest technology and security news when I saw an article about a new regulation. With new regulations coming out at a very rapid pace, it is difficult if not impossible to keep up with them. Where looking at them, they all have many things in common and that is that your IT environment needs to be as secure as it possibly can. Unfortunately there are differences in all of them that can be critical a company's reputation and financial status.

> "In April of 2002, hackers entered the California state government system and accessed personal information on over 200,000 state employees ranging from the governor to janitors. Worse yet, the government did not notify the employees until weeks after the incident occurred. SB 1386 was developed in response to this and similar breaches that have left hundreds of thousands of people victims of crimes they did not even know about. SB1386 is designed to ensure that Californians know any time their personal information may have been misappropriated. Those companies and agencies that do not comply with SB 1386, leave themselves vulnerable to civil lawsuits by anyone victimized by a security breach."[i]

I forwarded the information that I had found in this article to our Policy Compliance Marketing department to see we were working on any set of queries

for the Vulnerability Management software suite. After talking with the Windows Vulnerability Management Manager, I found that while we were aware of the new law, we did not have any new set of queries started for our customers to use.

I thought this would be an excellent case study for my SANS course and also wanted to see what steps it would take our customers to develop their own set of queries to report against their environment. The end result would also be a new set of queries for distribution on our company's website for customers to take advantage of so that it would help their environment be more secure. I was quickly volunteered/authorized to proceed.

2.0 Research of the Regulation

As I am not a lawyer, nor do I pretend to be one. I needed to understand what the law meant and how it would affect security on my windows environment. I started doing research on the web for new articles on SB 1386.

I quickly found the California Senate website and read about the bill. (See Appendix A: California Senate Bill 1386). I found most of the bill to talk about the security of data that personal information in it of California residents. If the data was breached, the company needs to contact the residents about it – UNLESS it is encrypted.

I attended the webinar sponsored by BindView on the "SB 1386: Lower Legal Liability and Cost:" with Joseph M. Burton Esq., in September. Mr. Burton is a California law firm partner of Duane Morris LLP and specializes in computer law.

The following facts were clarified for me:

"If you conduct business in California this applies to you. It does not matter if the business is physically outside of the state. What does matter is if you transact with customers from California."[ii] This law applies to all businesses, government agencies of California, but also to any business that has a California resident as a customer. This means that all internet businesses, mail order, etc could possibly be affected. It was no longer a local state problem. What this means is that if you are a company with servers that house data for other companies, you need to notify the housed company in case of breach of data.

"If you own or license computerized data that contains "personal information.

a. Personal information = 1798.82(e). The first name or first initial and last name in combination with one of the following:
    i. Social security number
    ii. Drivers license number
    iii. California ID account number
    iv. Credit card number or debit card number in combination with the password code
b. AND it is not encrypted. If both are encrypted, it is not personal data." [iii]

This Personal Information data would cover a lot of different areas. The need to search for these files became very crucial. Did Human Resources have resume files that have the name and social security number in it? What if you have password self service style programs that allow users to reset their passwords if they answered a set numbers of questions, and in that database was their user name and social security number. Did the user name equal their first and last name? Do I have in my Active Directory any fields that have this information in it – What about medical patient information? Insurance companies need this. If I am at a doctor's office, they request both my Social Security number and my Driver's license number- those data files on computer are now covered by this for California residents.
The crux of the bill is making sure that personal data is not breached. There are specific items that must be in a combination to make it personal data. If the first and last name and an important identifier are in the data, it is personal UNLESS they are encrypted. There is not any standard of encryption in this bill. The minimum of security encryption that I personally found acceptable was using Encrypted File System (EFS) and SSL. The data if kept in databases would need to be encrypted. Also. Unfortunately this will not be possible in all circumstances due to older systems in the environment and also some mission critical databases may not be able to be encrypted.

You must disclose any breach of the security of the system to the resident(s) of California. A breach was described as "Whose unencrypted personal information may be acquired by an unauthorized person. 1798.82(d) says that the breach of the security of the system is unauthorized acquisition of computerized data."[iv] This means that accessing and viewing the data is not clearly defined. But the acquisition of the data is a breach of security. The only way that I could help find a security breach would be by an extensive monitoring of the event logs to see if the security on my network has been changed from what my policies were, to see if I had patterns of login failures and more. I would need to continually check against changes to user permissions and rights, new groups and new machines in my environment. When I found these log entries or changes in the baselines of my reports, I would then need the ability to send the information to the people in charge of the objects to confirm the problem.

A good reference for policies and practices are covered in the "Recommended Practices for Protecting the Confidentiality of Social Security Numbers."
http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf
I would also recommend "Recommended Practices on Notification of Security Breach Involving Personal Information."
http://www.privacy.ca.gov/recommendations/secbreach.pdf
As both of these are written by the California government, their practices would be good information to base policies upon.

The California SB 1386 is only the start of this type of bill that has company's liable for personal information and holding them accountable to the people whose

data is on their machines. Most regulations before this has had the government liable for regulating and fining companies. In June 26, 2003, Diane Feinstien brought the NORPDA (Notification of Risk Personal Data Act) and it is in a Senate committee. “Yet with the exception of California, no State or Federal laws exist to require companies or government agencies to notify people if a hacker - or for that matter, another employee - breaks into the entities' database and compromises an individual's personal information.” [v]

An overview of what was needed to be able to report my windows environment

I already had an excellent vulnerability tool with many reports that covered most regulatory requirements from HIPAA and GLBA to the SANS top 20 Reports. What I needed was to create specific reports that took those into consideration but focused on the following key items from the SB 1386:

I am working on a test bed of Windows 2000 with Active Directory. I also have a second NT4.0 Domain. I am using BindView’s bv-Control for Windows to report on my environment. While I have a mixed environment of Linux, Novell, AD, and NT with Exchange, I am only going to query on the Windows environment for this case study. The queries that I will create will be able to be modified by anyone else using them. This means that I will leave the scoping (a way to just pick certain objects in the environment to report on) clear so that the customers can add this when they do their reporting.

Creation of Queries

I have created the reports using BindView’s bv-Control for Windows[vi]. All field, field descriptions, filtering, and sorting names are part of the product.

Where is the data located in my environment? I wanted to find the files that may have data in them. These could be anything from application documents in Human Resources, database files on web servers with credit card information, and sales customer information. Depending on the environment, I created reports that could be easily modifiable so that the customer could add their own file types to my queries, and also scope to where they knew the data files were after running the reports.

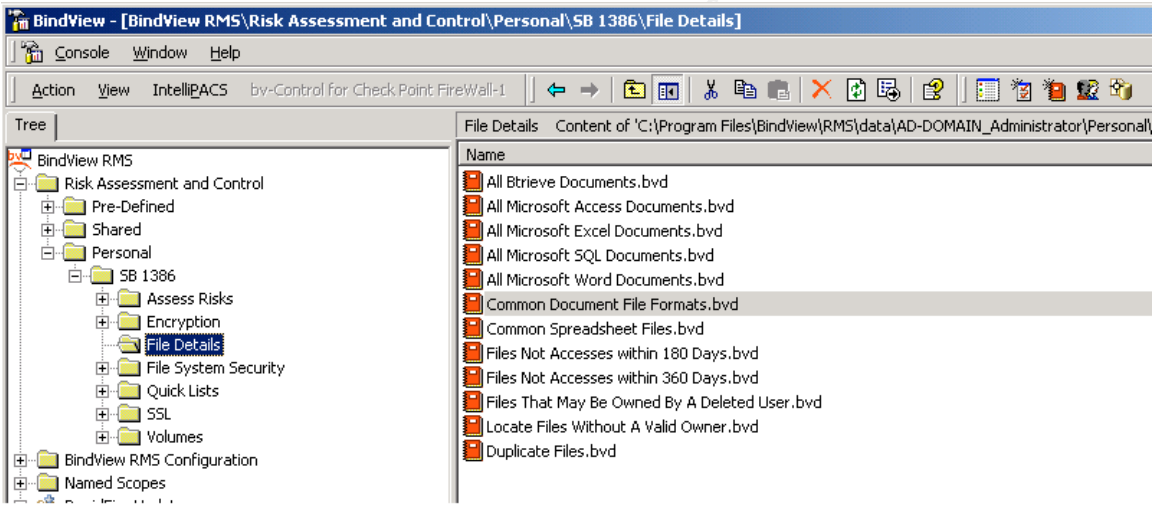

Figure 1: File Detail Reports[vii]

Where are my data files located?

The following reports all have the following fields (Domain/Workgroup Name, Machine Name, File Name (With Path), Last Accessed Date/Time, Owner, Owner SID is Valid?, and Size (Bytes)) so that you will know where the machine is, when it was accesses, and the owner. I broke them down into different types of files so that depending on the environment and depending on the software used at the company, they could easily get the information needed.

- *All Btrieve Documents* – Filtered with File Name (Extension only) Equal to .DAT
- *All Microsoft Assess Documents* – Filtered with File Name (Extension only) Equal to .LDB OR Filtered with File Name (Extension only) Equal to .MDB
- *All Microsoft Excel Document* - Filtered with File Name (Extension only) Equal to .XLS

- *All Microsoft SQL Document* - Filtered with File Name (Extension only) Equal to .LDF OR File Name (Extension only) Equal to .MDF.
- *All Microsoft Word Documents* - Filtered with File Name (Extension only) Equal to .DOC
- *Common Spreadsheet Files* – Filtered with File Name (Extension only) Matches Pattern .WK* OR File Name (Extension only) Matches Pattern .XL* OR File Name (Extension only) Matches Pattern.WQ* OR File Name (Extension only) Equal to .CSV OR File Name (Extension only) Equal to .DBF File OR Name (Extension only) Equal to .SLK or File Name (Extension only) Equal to .DIF.

Do I have duplicate files that may need to be deleted or cleaned up? This report can also be modified to add the filtering of what data type files I would be looking for, and also if you wanted to scope to a certain machine or directory, that is also customizable.

- *Duplicate Files* – Sort Specification of Only Allow Records with Duplicate Key selected on the File Name (Without Path)

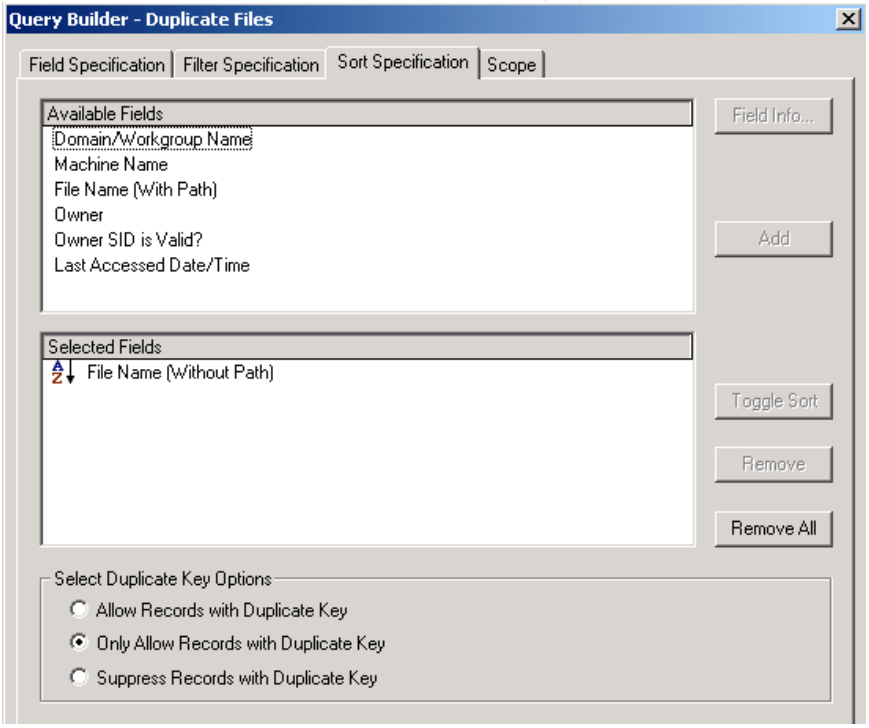

Figure 2: Showing Duplicate Key Option[viii]

Do I have data files that have not been access in a long time that possibly I could archive and get off of my network? Could I delete them? This is for the purpose of discarding unused personal information.

- *Files Not Accessed within 180 Days* – Filtered on Last Accessed Date/Time Days Before Today Less or Equal to 180

- *Files Not Accessed within 360 Days* - Filtered on Last Accessed Date/Time Days Before Today Less or Equal to 360

The next step would be to check with the owners to see if the files have California personal data in them. I need to make sure that I can get the owners. I also need to make sure that there are valid owners, and the owners are not deleted. The following reports have the following fields in them (Domain/Workgroup Name, Machine Name, File Name (With Path), File Name (Without Path), Creation Date/Time, Last Accessed Date/Time, Last Modified Date/Time.

- *Locate Files Without a Valid Owner* – Filtered on Owner SID is Valid? Is No

- *Files That May be Owned By a Deleted User* – Filtered on Owner SID is Valid? Is Not Yes AND Owner SID is Valid? Is Not [N/A] AND Owner SID is Valid? Is Not [Locked]

It would be better for me to centralize these data files so that I would have a better control of the security. By using the previous reports, I could find the reports and then be able to find a better place for the files. An educational program will definitely need to happen so that employees will know why we are looking at the files. I would recommend using the "Recommended Practices for Protecting the Confidentiality of Social Security Numbers" to get ideas of how to phrase the policies.
http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf

Who has access to this data?
Using the Principle of Least Privilege I need to check to see if "the default NTFS permission is Full Control for the Everyone group; that is to say, the default NTFS DACL is the worst possible from a security standpoint."[ix] With the combination share and NTFS permissions, I need to find effective permissions on the Shares, Directories and if needed files.

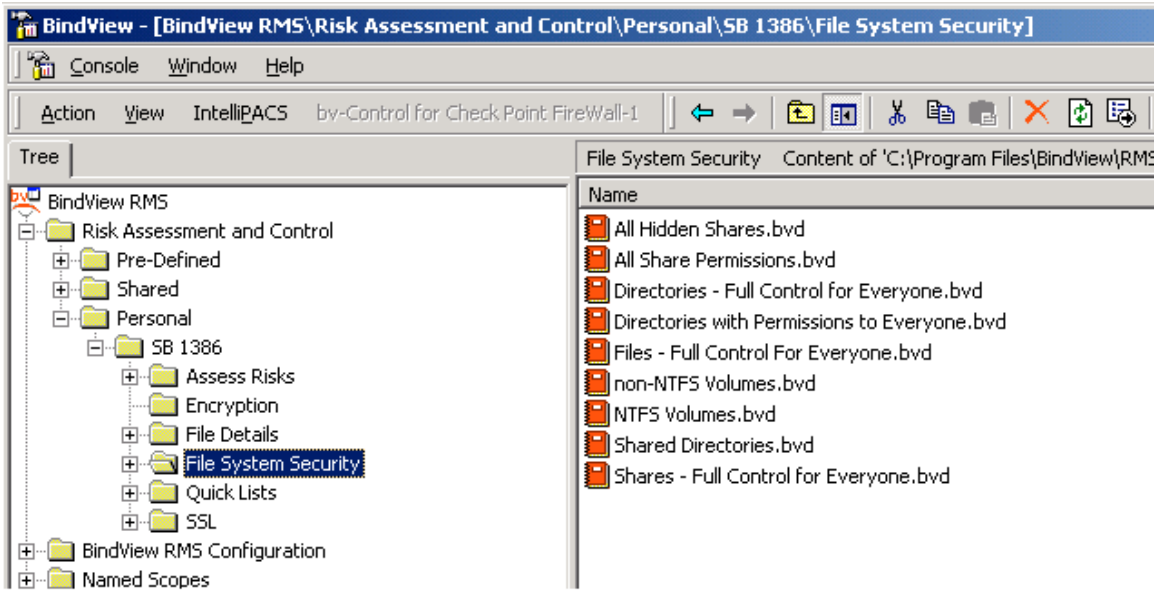

Figure 3: File System Reports[x]

I need to make sure that my volumes are NFTS so that I can take advantage of Windows security. If I find that any data is on a non-NTFS volume, it will need to be changed immediately.

- *Non- NTFS Volumes* – Filtered on Is NTFS? Is Not Yes. Fields include (Domain/Workgroup Name, Source Machine, Volume Name, File System Type).
- *NTFS Volumes* – Filtered on Is NTFS? Is Yes. Fields include (Domain/Workgroup Name, Source Machine, Volume Name, File System Type).

I need to find out who has access and permissions to the shares, directories, and files. If the data is in a database, I need to make sure that the users having access are valid and secure.

First I will be looking at the shares and have reports on all permissions, but looking also for hidden shares and the ones that have group everyone with full control.
The following reports have fields of (Domain/Workgroup Name, Machine Name, Share Name, Is Hidden?, Permissions).

- *All Share Permissions* - No filtering
- *All Hidden Shares* - Filtered on Is Hidden? Is Yes
- *Shares – Full Control for Everyone* – Filtered on Permissions <Form> Contains Everyone Full Control. Fields include (Domain/Workgroup Name, Machine Name, Share Name, Share Path, Type of Object Being Shared, Permissions

Checking at the directory level with reports that are concentrating on the everyone group. The following reports have the following fields (Domain/Workgroup Name, Machine Name, Directory Name, Is Shared?, Permissions)

- *Directories – Full Control for Everyone* – Filtered on Permissions Match? “”\Everyone”,”1”,”ALL”,”1”,”ALL” is Yes
- *Directories with Permissions to Everyone* - Filtered on Permission <FORM> Contains Everyone.

Although it is not the best practice of assigning permissions on the files level, I still want to confirm that the filterable and scopable files do not have everyone with full control.

- *Files – Full Control for Everyone* - Filtered on Permissions Match? “”\Everyone”,”1”,”ALL” is Yes. Fields included are (Domain/Workgroup Name, Machine Name, File Name (With Path), Owner, Last Modified Date/Time, Last Accessed Date/Time, Permissions).

Check for Encrypted File System

With the possibility of traveling data, I want to make sure that the computers have Encrypted File System (EFS). The reason is so that if my physical security is breached and someone tries to copy the file, it will be encrypted. EFS Implementation requires Windows 2000 service pack 2 as the minimum configuration. I want to make sure that all of my machines that are storing the data has at least this OS and service pack so that they can take advantage of the EFS.

The first thing to do is to find out what OS’s I have out there. I also need to compare if these machines are those that have the data files I discovered previously. The following reports all have the following fields (Domain/Workgroup, Name, Machine Name, OS Version String, OS Service Pack Revision).

- *NT4 Machines* – Filtered on OS Version String Contains 4.0
- These are machines I definitely want to move data from if possible.
- *Windows 2000 Workstations* – Filtered on OS Version String (Browser) Contains 5.0 AND Machine is Workstation? (Browser) Is Yes
- *Windows 2000 Servers* - Filtered on OS Version String (Browser) Contains 5.0 AND Machine is Server? (Browser) Is Yes AND OS Version String (Browser) Doesn’t Contain 3.5
- *Windows XP Professional* - Filtered on OS Version String (Browser) Contains 5.1 AND Machine is Server? (Browser) Is No
- *NT5 Machines not up to service pack 2* –Filtered on OS Versions String Contains 5.0 AND (OS Service Pack Revision Less than Service Pack 2 OR OS Service Pack Revision Is (Not Accessible))

The next step is to confirm that common document folders are encrypted with EFS. This will include "My Documents" folder, %TEMP%, and the Local print spool folder is encrypted".[xi]

- *Directories with EFS Turned on* – Filtered on Attributes <LIST> Contains {E} Fields included are (Domain/Workgroup Name, Machine Name, Directory Name, Attributes <LIST>)
- *Personal Directories without EFS Turned on* -– Filtered on Attributes <LIST> does not Contain {E} AND (Directory Name (Without Path) Contains My Documents OR Directory Name (Without Path) Contains Temp))
- *Temp Directories without EFS Turned on*

Data base files could take advantage of the encryption turned on.

- *Files with Encryption turned on* – Filtered on Attributes <LIST> Contains {E} Selected Fields are (Domain/Workgroup Name, Machine Name, File Name (With Path), Attributes <LIST>).
- *Machines with CIPHER.EXE* – Filtered on File Name (Without Path) Equal to CIPHER.EXE. Fields included are (Domain/Workgroup Name, Machine Name, File Name (with Path).

Are the databases/files internally encrypted? There is not a way for me to tell with my reports. I will need to contact the data owners to confirm this.

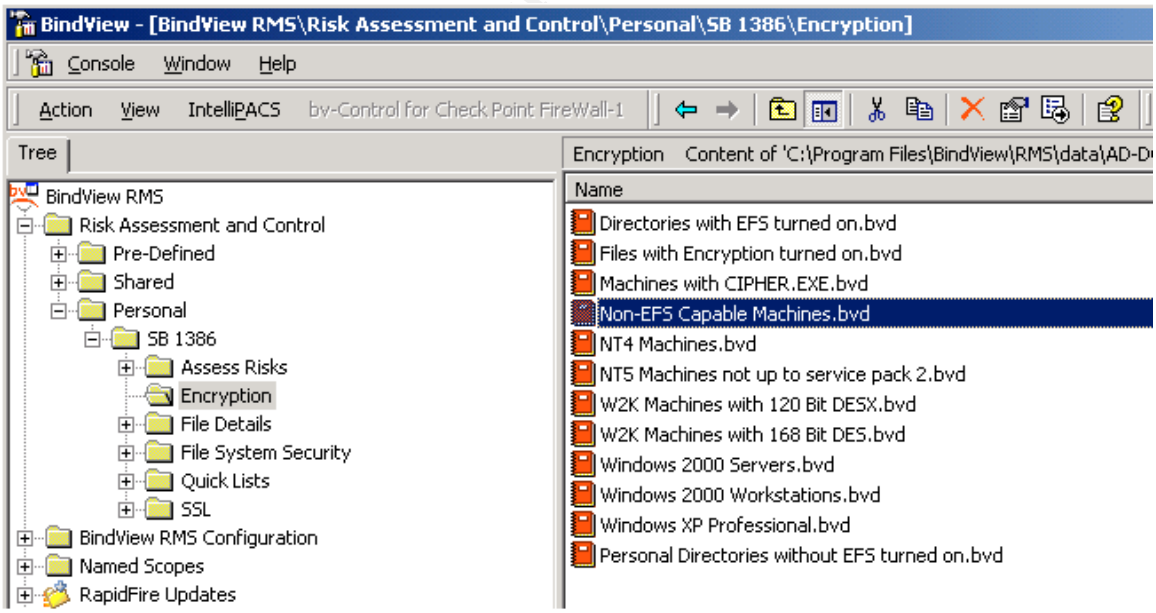

Figure 4: Encryption Reports[xii]

Can I tell if it has been breached?

Do I have auditing turned on? I will need to confirm that this is at all locations of the data that has been identified as vulnerable. I used the Assess Risks Reports that report on the event logs for the following reports on the security and system event logs.

An excellent source for understanding what the event ids are "Windows 2000 Common Criteria Secure Configuration Guide, Appendix B - Audit Categories and Events located at the TechNet section of Microsoft's web site. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/issues/W2kCCSCG/W2kSCGcb.asp

Event Logging/Policy Change
The following Reports are run against the Security Event Logs on
Fields included are (Domain/Workgroup Name, Event Date/Time, Machine Name, Source, User Name).

- *Add or Remove Trusted Domains* – Filtering on Security Event ID's Equal to 610 or 611
- *Audit Policy Change*- Filtering on Security Event ID Equal to 612
- *Domain Policy Changed* - Filtering on Security Event ID Equal to 643
- *User Right Assigned or Changed* - Filtering on Security Event ID Equal to 608 or 609
- *User Rights or Audit Policy Changed* - Filtering on Security Event ID Equal to 608 OR 609 OR 612 OR 626

System Events
The following Reports are run against the System Event Log. Fields include (Domain/Workgroup Name, Event Date/Time, Machine Name, Source)

- *Audit Event Records Discarded* – Filtering on System Event ID Equal to 516
- *System Audit Log Cleared* - Filtering on System Event ID Equal to 517
- *System Restart* - Filtering on System Event ID Equal to 512

User and Group Management - The following Reports are run against the Security Event Log. Fields include (Domain/Workgroup Name, Event Date/Time, Machine Name, Source, Event Description).

- *Change Password Attempt* - Filtering on Security Event ID Equal to 627
- *Failed Logon – Account Locked out* - Filtering on Security Event ID Equal to 539
- *Local or Global Group Member Added* - Filtering on Security Event ID Equal to 536
- *Logon Failure for Guest Account* - Filtering on (Security Event ID Equal to 531 OR 529) AND Security Event Description (SIDs Expanded)<FORM> Contains Guest
- *New User Created and_or Rights changed* - Filtering on (Security Event ID Equal to 624 OR 625 OR 642) AND User Name is inputted by User

- *User Account Changed* - Filtering on Security Event ID Equal to 642

Violations of Accounts Policies The following Reports are run against the Security Event Log. Fields include (Domain/Workgroup Name, Event Date/Time, Machine Name, Source, Event Description).

- *Failed Logon – Disabled Account* - Filtering on Security Event ID Equal to 531
- *Failed Logon – Expired Account*- Filtering on Security Event ID Equal to 532
- *Failed Logon – Logon Type Restricted*- Filtering on Security Event ID Equal to 534
- *Failed Logon – Password Expired*- Filtering on Security Event ID Equal to 535
- *Failed Logon – Time Restriction Violation*- Filtering on Security Event ID Equal to 530
- *Failed Logon – Unknown Username or Bad Password*- Filtering on Security Event ID Equal to 529
- *Failed Logon – User Not Allowed to Log On*- Filtering on Security Event ID Equal to 533
- *Failed Logon*- Filtering on Security Event ID Equal to 537

Windows 2000 Security Events The following Reports are run against the Security Event Log. Fields include (Domain/Workgroup Name, Event Date/Time, Machine Name, Source, Event Description).

- *Encrypted Data Recovery Policy Changed*- Filtering on Security Event ID Equal to 617
- *IPSec Policy Agent Changed*- Filtering on Security Event ID Equal to 615
- *IPSec Policy Agent Disabled*- Filtering on Security Event ID Equal to 614
- *IPSec Policy Agent Potential Failure*- Filtering on Security Event ID Equal to 616

User Access Rights

By knowing what is out in my environment with the users and permissions that they have, I can use the following reports to baseline and document the information. During the process of baselining, I can also check on items that have changed and allow me to know what has been affected, alerting me on occurrences that I may or may not have set up auditing for.

Profile Information

- *All User Account Profile Information* – Fields include (Domain Name, Profiles: Users Without, Profiles: Users With Invalid (This field returns a list of users with profiles that cannot be accessed. This usually indicates that the path specified for the user's profile is incorrect, or the security on the directory is preventing validation.), Profiles: Users with Mandatory, Profiles: Users with Personal)
- *User Accounts with a Mandatory Profile* - Fields include (Domain Name, Profiles: Users with Mandatory).
- *User Accounts with a Personal Profile* - Fields include (Domain Name, Profiles: Users with Personal).

Group Information

- *Detailed Group Analysis and Documentation* – Fields include (Domain/Workgroup, Machine Name, Fully Qualified Name, Group Memberships: Domain Global, Effective Group Memberships with descriptor, Group Memberships: Server Operator?, Group Memberships: Print Operator, Group Memberships: Account Operator, Group Memberships: Total Domain Global).
- *Domain Global Groups* – Fields include (Domain Name, List of Global Groups).
- *Domain Local and Global Groups* - Fields include (Domain Name, List of Local Groups, List of Global Groups).
- *Domain Local Group Membership Analysis* – Fields include (Domain/Workgroup, Machine Name, Fully Qualified Name, Effective Member Analysis – This field returns all of the effective members (users, machines, and special built in groups such as Everyone, Batch, Authenticated Users, Dialup…) of the group and how each obtained their membership in the group). This is filtered on Group is Domain Local? Is Yes.
- *Domain Local Groups* - Fields include (Domain Name, List of Local Groups).
- *Effective Admin Group Members* – Fields include (Fully Qualified Name, Effective Members and is Filtered on Group Name Contain Admin).
- *Group Membership Analysis* - This is a difficult report to get using native tools. Fields include (Domain/Workgroup Name, Machine Name, Fully Qualified Name, Effective Member Analysis -This field returns all of the effective members (users, machines, and special built in groups such as Everyone, Batch, Authenticated Users, Dialup…) of the group and how each obtained their membership in the group).

User Information

- *Domain Users, Local and Global Groups* - Fields include (Domain Name, List of Users, List of Local Groups, List of Global Groups).
- *Domain Users* – Fields include (Domain Name, List of Users).
- *Enabled Guest Accounts* – Fields include (Domain/Workgroup Name, User Name, Account Privilege Level, Account Description, Password Expires? (Effective), Station Restrictions). Filters are User Name Equal To Guest AND Account Disabled? Is Not Yes.

User Rights and Permissions

- *Excessive User Rights*– Fields include (Domain/Workgroup, Machine Name, Users with the Right To Act as part of the operating system or Take ownership of files or other objects or Back up files and directories or restore files and directories or Shut down the system).
- *Machine Default Accounts* - Fields include (Domain/Workgroup Name, Machine Name, Administrator Account Name, Accounts: Administrator Account Renamed? Guest Account Name, Accounts: Guest Account

Renamed?) This report is checking to see if I have renamed the machine default accounts.

- *Permissions List on Sensitive Directories* -Fields include (Domain/Workgroup, Machine Name, Directory Name, Permissions (Advanced)).
- *Permissions List on Sensitive Shares*-Fields include (Domain/Workgroup, Machine Name, Share Name, Permissions).
- *User Account Maximum Privilege Level* – Fields include (Domain/Workgroup Name, User Name, Full Name, Account Privilege Level – The field returns the privilege level indicating a user's highest group membership (Guest, User, Admin) on the machine where the user's account was created, Administrator Equivalent?).
- *User Account Station and Time Restrictions* – Fields include (Domain/Workgroup Name, User Name, Station Restrictions Exist?, Station Restrictions, Time Restrictions).
- *User Accounts with RAS Settings Enabled* – Fields include (Domain/Workgroup Name, User Name, Full Name, RAS Callback Activated?, RAS Callback Number, RAS Callback Preset?, RAS Callback Set By Caller?, RAS Dialin Allowed?). This is filtered on RAS Callback Activated? Is YES AND (RAS Callback Preset? Is Yes OR RAS Callback Set By Caller? Is Yes) AND RAS Dialin Allowed? Is Yes.
- *User Rights Report* - Fields include (Domain/Workgroup Name, Machine Name, User Rights – This field returns a listing of each system privilege (user right) on a machine and the accounts that have been grated those privileges. This provides an easy means of documenting the privilege assignments for a machine.)

Trust Information

- *Domain Trust Information* – Fields include (Domain Name, Trusted Domains , Trusted Domains: Verified, Trusted Domains: Broken, Trusting Domains, Trusting Domains: Verified, Trusting Domains: Broken).
- *Verified Domain Trusts* – Fields include (Domain Name, Trusted Domains , Trusted Domains: Verified, Trusting Domains, Trusting Domains: Verified).

Submission of the results to Marketing

The queries have been submitted to the marketing managers. My part of the procedure is complete. They will now take them and possibly revise or add to them. All of the reports will be sent through an extensive quality assurance process to confirm operability on various OS's. I hope to see them soon posted on our customer portal website so that customers can use them. Product Marketing is currently working on policies and procedures to help customers in their continual task of improving overall security and restricting access of personal information. They are in progress of a matrix for SB 1386 that will soon be published to our web site.

Summary
The exercise of creating the queries looking for data that might be affected for a company using BindView's bv-Control for Windows vulnerability management software showed me that while it was very easy to create new queries to look for new regulations like the California SB 1386, the difficult part was the research.

I researched on what was unique about the regulation, and through this was able to focus on the data files that might contain personal information of California residents. Although I was not able to guarantee that the databases or files were internally encrypted, but by locating possible files, I could limit the locations to which the files were residing on. In doing this, I could segregate the personal information to systems that were not as susceptible to attack. I could discard unneeded personal information files, or archive them off of the network and store them in a secure locked area. Finding the files I was able to restrict the authorized access to them by confirming the permissions of shares, directories and even files. I further ensured security by adding the layer of Encryption File System to any location of the data files.

With continual diligence of the auditing and watching of the security logs I have set up a way to be able to establish response and though policies have a good notification procedure. The queries that were created show also that it is possible to continually update what I look for in my environment in regards to security and regulations.

I realize that this is just one of the regulations that companies have to take into consideration when improving their overall security. The queries that I created are just part of the continual assessment that needs to be done on networks, but it is a compliment to the other parts of the bv-Control to Windows product. By using this tool with others, it will be easier to control the security.

The SB 1386 is only a start. By getting secure now you will be able to be ready for the NORPDA or other legislation like it. "This bill has a tough but fair enforcement regime, and will give ordinary Americans more control and confidence about the safety of their personal information," Senator Feinstein said. "Americans will have the security of knowing that should a breach occur, they will be notified and be able to take protective action." [xiii]

Appendix A: California Senate Bill 1386
"BILL NUMBER: SB 1386CHAPTERED
BILL TEXT

CHAPTER 915
FILED WITH SECRETARY OF STATE SEPTEMBER 26, 2002
APPROVED BY GOVERNOR SEPTEMBER 25, 2002
PASSED THE SENATE AUGUST 30, 2002
PASSED THE ASSEMBLY AUGUST 26, 2002
AMENDED IN ASSEMBLY AUGUST 23, 2002
AMENDED IN ASSEMBLY AUGUST 5, 2002
AMENDED IN ASSEMBLY JULY 25, 2002
AMENDED IN ASSEMBLY JUNE 30, 2002
AMENDED IN ASSEMBLY JUNE 20, 2002
AMENDED IN ASSEMBLY JUNE 6, 2002
AMENDED IN SENATE MARCH 20, 2002

INTRODUCED BY Senator Peace
(Principal coauthor: Assembly Member Simitian)

FEBRUARY 12, 2002

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 1386, Peace. Personal information: privacy.

Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law also requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records. Existing law provides civil remedies for violations of these provisions.

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. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation.

The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill would state the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. (a) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector.

(b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet Web sites are all sources of personal information and form the source material for identity thieves.

(c) Identity theft is one of the fastest growing crimes committed in California. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities. The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108 percent increase over the previous year's caseload.

(d) Identity theft is costly to the marketplace and to consumers.

(e) According to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative.

SEC. 2. Section 1798.29 is added to the Civil Code, to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal

investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized aquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 3. Section 1798.82 of the Civil Code is amended and renumbered to read:

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

SEC. 4. Section 1798.82 is added to the Civil Code, to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 5. This act shall become operative on July 1, 2003.

SEC. 6. This act deals with subject matter that is of statewide concern, and it is the intent of the Legislature that this act supersede and preempt all rules, regulations, codes, statutes, or ordinances or all cities, counties, cities and counties, municipalities, and other local agencies regarding the matters expressly set forth in this act. "[xiv]

Appendix B – Additional References for SB1386 and Security

"Recommended Practices for Protecting the Confidentiality of Social Security Numbers." June 2002; revised January 2003.
http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf

"Recommended Practices on Notification of Security Breach Involving Personal Information." October 2003.
http://www.privacy.ca.gov/recommendations/secbreach.pdf

"Threat Profiling Microsoft SQL Server (A Guide to Security Auditing). July 2002.
http://www.ngssoftware.com/papers.html

"HOW TO: Manage the Encrypting File System in Windows Server 2003 Enterprise Server." http://support.microsoft.com/default.aspx?scid=kb;en-us;324897

"Encrypting File System: Your Secrets are Safe."
http://www.microsoft.com/windows2000/techenthusiast/features/efs.asp

"Step-by-Step Guide to Encrypting File System (EFS)."
http://www.microsoft.com/windows2000/techinfo/planning/security/efssteps.asp

References:

All BindView bv-Control for Windows Queries including report names, query field, filtering, sorting and scooping information:
"BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179.
http://www.bindview.com
http://www.bindview.com/Products/VulnMgmt/AssesmentandSecurity/bv-Control_Windows.cfm
http://www.bindview.com/resources/Datasheets/bvCWinActiveDirDS.pdf

All Microsoft Windows Event ID numbers:
"Windows 2000 Common Criteria Secure Configuration Guide, Appendix B - Audit Categories and Events"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/issues/W2kCCSCG/W2kSCGcb.asp

Levack, Kinley. "SB 1386: How California Wants to Keep Your Secrets." July 1, 2003.
http//www.econtentmag.com/Articles/ArticlePrint.aspx?ArticleID=4624&CategoryID=14

Burton, Joseph M. Esq. "SB 1386: Lower Legal Liability and Cost." September 17, 2003. Webinar http://www.bindview.com/events/GetEvents.cfm?NUM=927

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

Cole, Eric, Fossen, Jason, Northcutt, Stephen, Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1. The SANS Institute. 2003

Bill Number: SB 1386 Chaptered Bill Text,
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

---

[i] Levack, Kinley. "SB 1386: How California Wants to Keep Your Secrets." July 1, 2003.
http//www.econtentmag.com/Articles/ArticlePrint.aspx?ArticleID=4624&CategoryID=14

[ii] Burton, Joseph M. Esq. "SB 1386: Lower Legal Liability and Cost." September 17, 2003. Webinar http://www.bindview.com/events/GetEvents.cfm?NUM=927

[iii] Burton, Joseph M. Esq. "SB 1386: Lower Legal Liability and Cost." September 17, 2003. Webinar http://www.bindview.com/events/GetEvents.cfm?NUM=927

[iv]Burton, Joseph M. Esq. "SB 1386: Lower Legal Liability and Cost." September 17, 2003. Webinar http://www.bindview.com/events/GetEvents.cfm?NUM=927

[v] "Senator Feinstein Seeks to Ensure Individuals are Notified when Personal Information is Stolen from Databases." June 26, 2003. http://www.senate.gov/~feinstein/03Releases/datasecurityrelease.htm

[vi] BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179. http://www.bindview.com

[vii] "BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179. http://www.bindview.com

[viii] "BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179. http://www.bindview.com

[ix] Cole, Eric, Fossen, Jason, Northcutt, Stephen, Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1. The SANS Institute. 2003. P-1186 .

[x] "BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179. http://www.bindview.com

[xi] Cole, Eric, Fossen, Jason, Northcutt, Stephen, Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1. The SANS Institute. 2003. P-1201.

[xii] "BindView RMS Console", BindView Corporation. Version 7.2.3086 Service Pack 3. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 7.3.179. http://www.bindview.com

[xiii] "Senator Feinstein Seeks to Ensure Individuals are Notified when Personal Information is Stolen from Databases." June 26, 2003. http://www.senate.gov/~feinstein/03Releases/datasecurityrelease.htm

[xiv]Bill Number: SB 1386 Chaptered Bill Text, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html