Tape Vaulting Audit And Encryption Usage Analysis

Prepared for Public Presentation

(includes "SB 1386", "Gramm Leach Bliley", and "Personal Data Protection and Security Act of 2005" Customer Information Protection and loss reporting requirements review and analysis)

Presented by:

Tom Bronack,

Phone: (718) 591-5553

Email: bronackt@dcag.com

Abstract

- Loss of media events have happened frequently and could result in Identify Theft to customers whose information was on lost media or exposed to data breach.
- Potential monetary losses are great for company and individuals, through civil charges, and potentially criminal charges.
- Personal Data Privacy and Security Act of 2005; Gramm, Leach, Bliley (GLB); and CA State Bill 1386 all require that customers be immediately informed of a data breach or lost media event.
- The cost associated with the Tape Vaulting Audit and Encryption Usage Analysis engagement is very small in relationship to the amount that can be lost.
- Project identifies Gaps and Exposures and results in implemented Procedures and Response Plans that help the organization adhere to laws and regulations in a controlled manner.
- Better customer safeguards though controls, procedures, and response plans.

ChoicePoint losses due to Personal Data Breach

- Fined $15 million by FTC.
- Lost 25% market cap, or $750 million.
- Lost $15-20 million in Core Revenue.
- Lost 10-20 cents per share.
- Spending $2 million on credit bureau memberships for customers affected by data breach.
- Will suffer more scrutiny in the future.
- Will never regain reputation lost due to data breach.

Goals and Objectives

- Review Laws and Regulations affecting Tape Transport To/From data center and remote locations.
- Review the Tape transportation process between the data center and remote locations (i.e., Vaults, Customers, Credit Bureaus, other).
- Evaluate vendors included in the media transportation process, including those used for purchase and disposal of media.
- Perform an Audit of the Local and Remote Vaults.
- Research existing Insurance over loss of media.
- Review Procedures and the Response Plan for lost media or a Data Breach.
- Investigate the use of Encryption to protect data from misuse.
- Identify Exposures and Gaps, define impact, draw conclusions, and make recommendations to mitigate and remedy identified problems.
- Prepare a Final Report with findings and recommendations.

Gramm Leach Bliley Safeguard Rule

- **Effective – May 23, 2002**
- **Covered Entities include - Financial institutions as defined in the Bank Holding Company Act that possess, process, or transmit private customer information.**
- **Purpose – Protect Customer Information from unauthorized disclosure or use.**
- **Operative Mechanisms – Information Security Program:**
  - **Responsible Employee Selection and Assignment;**
  - **Risk Assessment performed;**
  - **Information safeguards and controls implemented;**
  - **Oversight of "Service Providers"; and**
  - **Testing and Monitoring.**
- **Criminal Consequence of Non Compliance – Fines and imprisonment of up to Five (5) years.**

California SB 1386 (State Bill)

- California SB 1386 became effective on July 1, 2003, amending civil codes 1798.29, 1798.82 and 1798.84. It is a serious bill, with far reaching implications.
- Designed to force any public or private entity that maintains electronic customer data to report the misuse, loss, or destruction of such data immediately upon the discovery.
- Purpose is to reduce, or eliminate, personal identify theft.
- Essentially, it requires an agency, person, or business entity that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).
- If company's fail to notify, they will be subject to civil penalties and suit by each of the people who have had their identity records compromised.
- In order to reduce or eliminate the potential for media loss during transport, the Tape Vaulting Audit and Encryption Usage Analysis engagement has been requested.
- This engagement will review how media is presently transported between the data center and remote locations, vendor operations, and the potential use of Encryption. Making recommendations to eliminate exposures and gaps.

Personal Data Privacy And Security Act of 2005

- **Designed to replace California SB 1386 nationwide.**
- **Introduced by Sen. Arlen Specter (R-Pa.) and Sen. Patrick Leahy (D-Vt.)**
- **Key Features include:**
  - **Requires companies that have databases with personal information on more than 10,000 Americans to establish and implement data privacy and security programs, and vet third-party contractors hired to process data;**
  - **Increasing criminal penalties for identity theft involving electronic personal data by (1) increasing penalties for computer fraud when such fraud involves personal data, (2) adding fraud involving unauthorized access to personal information as a predicate offense for RICO and (3) making it a crime to intentionally or willfully conceal a security breach involving personal data;**
  - **Giving individuals access to, and the opportunity to correct, any personal information held by data brokers;**
  - **Requiring entities that maintain personal data to establish internal policies that protect such data and vet third-parties they hire to process that data;**

Personal Data Privacy And Security Act of 2005 *continued*

- Key Features include: *continued*

  - **Requires notice to law enforcement, consumers and credit reporting agencies when digitized sensitive personal information has been compromised. The trigger for notice is tied to risk of harm, and there are exemptions for notice where the risk is *de minimis* or where fraud prevention techniques prevent harm to consumers. Also requires that companies provide victim protection assistance, specifically free access to credit reports and credit monitoring services, to individuals notified that their personal data has been breached ;**

  - **Limits the buying, selling or displaying of a social security number without consent from the individual whose number it is, prohibits companies from requiring individuals to use social security numbers as their account numbers and places limits on when companies can force individuals to turn over those numbers in order to obtain goods or services, and bars government agencies from posting public records that contain Social Security numbers on the Internet; and**

  - **Requiring the government to establish rules protecting privacy and security when it uses data broker information, to conduct audits of government contracts with data brokers and impose penalties on government contractors that fail to meet data privacy and security requirements.**

Defining a GLB or 1386 type of violation

- **These guidelines are the only ones requiring notification if a "Breach" occurs, whether it be electronic or paper.**
- **Combination of "Sensitive" Customer Information, including:**
  - ***Name, Address, Telephone Number, PLUS***
  - ***Social Security Number, Account Number, Credit / Debit Card Number and associated PIN, or any combination of components that would allow access to individuals account.***
- **States that are enacting similar bill as 1386 include:**

Arkansas	Louisiana	North Carolina
Connecticut	Maine	North Dakota
Delaware	Minnesota	Rhode Island
Florida	Montana	Tennessee
Georgia	Nevada	Texas
Illinois	New Jersey	Washington
Indiana	New York	Maybe Federal

Companies experiencing a 1386 or GLB Breach include:

ABN Amro Mortgage Group	CitiGroup, Inc	People's Bank
Ameritrade Holding Corp.	Dept. of Justice	Several Universities
Bank of America Corp.	Ford Motor Company	Time Warner
CardSystems Solutions, Inc.	HSBC North America	Sam's Club – a division of Wal Mart
Choicepoint, Inc	Marriott Corporation	American Express

I have developed a Tape Vaulting Audit and Encryption Analysis Engagement to help customers respond to these laws and to increase their protection over critical client information. Contact me if you are interested.

Tape Vaulting Audit

- **Define Scope and Deliverables:**
  - **Define off-site locations receiving media, including:**
    - **Remote Vendor Vaults;**
    - **Credit Bureaus; and**
    - **Customers, etc.**
  - **Evaluate Backup and Vaulting Procedures.**

- **Define Goals and Objectives:**
  - **Identify media to be safeguarded during transport to/from remote locations;**
  - **Review and Optimize procedures governing media transport;**
  - **Review and suggest methods for optimizing protection for media being transported between locations; and**
  - **Recommend updates to standards and Procedures, as needed.**

Project Phases and Assignments

- **Assign Team Members**
  - **Define functions to be performed;**
  - **Select personnel with required skills to perform functions;**
  - **Assign personnel to project functions;**
  - **Establish schedule for periodic reviews (Communication Plan);**
  - **Review project purpose and deliverables with team members;**
  - **Gain consensus with team members;**
  - **Agree upon deliverables and schedule (Detailed Work Program); and**
  - **Develop Action Plan for team members.**

Environment Overview

- **Define locations included in study, such as:**
  - **Data Centers, Remote Vaults, and Credit Bureaus;**
  - **Other locations.**
- **Define Operating Systems Used.**
- **Define Tape Management Systems Used.**
- **Review Tape Management Organization and Staff.**
- **Review Staff Functional Responsibilities.**
- **Review Staff Job Descriptions.**
- **Review Tape Management Standards and Procedures Manual.**

External Relationship Review

- **Define Vendor Relationships:**
  - **Vaulting; and**
  - **Media purchase and disposal.**
- **Review Vendor Contracts.**
- **Review insurance related to media loss.**
- **Review company response to media loss (CA 1386).**
- **Review media re-use and disposal policies and practices.**

Selecting Media for Backup and Vaulting

- **Review Vital Records Management procedures:**
  - **Identifying files for backup and vaulting;**
  - **Determining the best time to perform backups;**
  - **Review vaulting procedures; and**
  - **Discuss operations with management and staff.**
- **Review file naming conventions.**
- **Review Standards and Procedures for this area of work.**
- **Review vaulting schedule and past history.**

Review How Backups are Created

- **Review Operating System requirements.**
- **Review Tape Management System.**
- **Review Backup Job Stream and Schedule:**
  - **Weekly and Monthly backup schedule;**
  - **Daily Incremental Backups;**
  - **Other types of backup; and**
  - **Backup Schedule as it relates to production schedule.**
- **Review physical movement of media to backup machine and then to storage area in preparation for vaulting company pickup.**
- **Review Backup logs, tracking, and reporting for both customer and remote location to synchronize file location.**

Review Media Transportation Procedures

- **Define where media is stored before pick-up.**
- **Determine if the location is secure.**
- **Review Vault Management System and its usage.**
- **Review vaulting procedures for:**
  - **Local Vault;**
  - **Customer off-site vault; and**
  - **Vendor off-site vault.**
- **Review associated standards and Procedures Manual sections relating to the above operation.**

Audit Vaulting Vendor Location and Procedures

- **Review pickup and delivery procedures.**
- **Review log-in and log-out procedures.**
- **Review how media is packed, shipped, and received at vendor location.**
- **Review vendor procedures when receiving media for vaulting.**
- **Review Vault Management System and its reports.**
- **Review any methods for customer to validate vaulted media has arrived and is placed in storage rack via remote access or hard copy reports.**
- **Identify Gaps and Exposures associated with process and documentation.**
- **Compare process with other vendors.**

Evaluate Current Vaulting Procedures

- **Evaluate findings and documentation.**
- **Identify Gaps and Exposures.**
- **Rate impact of Gaps and Exposures.**
- **Make recommendations for improvement.**
- **Prepare supportive documentation to make it easier for the customer and vendor to more easily correct mistakes.**
- **Present findings to customer for review.**
- **Make any changes deemed necessary.**
- **Create final media vaulting evaluation document.**

Evaluate the Need for Encryption

- **Define the types of files that are candidates for Encryption, including:**
  - **Long-term files may not be good candidates.**
  - **Short-term sensitive files may be excellent candidates.**
  - **Financial, Compliance, and other critical files.**
- **Define and research the Types of Encryption available:**
  - **Encryption Key Methodology (128 bit, etc.).**
  - **Encryption Key escrow and usage procedures.**
  - **Duration associated with Encryption Jobs and their impact on production schedules.**
  - **Define Encryption Selection and Usage criteria.**

Final Report

- **Management Report.**
- **Management Presentation.**
- **Discussion of Findings.**
- **Working with the customer after final report.**
- **Where do we go from here.**