IBM/Tivoli

To Tell The Truth:
State Data Breach Notification Laws

Marne E. Gordan

GRC Market Manager

Agenda

- When Bad Things Happen to Virtual People
- Notification Laws
  - Federal
  - State
- InfoSec and the Myth of Encryption
- Fix, Prosecute or Notify ?
- Summary
- Q&A

IBM/Tivoli

When Bad Things Happen to Virtual People

The Exponential Rise in ID Theft

At the Seattle Cancer Care Alliance

- **Patient Eric Drew's identity stolen by phlebotomist Richard Gibson**
  - Gibson had access to patient record
  - Obtained Drew's SSN, date of birth, and primary address
  - Used this information to open lines of credit
  - Ran up over $9k in debt
    - Clothing
    - Jewelry
    - X-Box
    - Porcelain figurines

http://www.msnbc.msn.com/id/10549098/

Drew Began Receiving Unsolicited Mail/Collection Notices

- **Contacted major credit bureaus**
  - Placed fraud warnings on legitimate credit cards
  - Begged major issuers not to issue any new cards
  - Contacted local law enforcement
- **Nothing happened, until**
  - Local reporter Chris Daniels at KING-5 NBC TV reported the story
  - Daniels and Drew continued the investigation
  - Forensic trail led to Gibson
- **Gibson plead guilty**
  - 16 months in jail, plus restitution
  - First documented “HIPAA conviction”
  - **Convicted of unlawful use of IIHI**

From the Federal Trade Commission

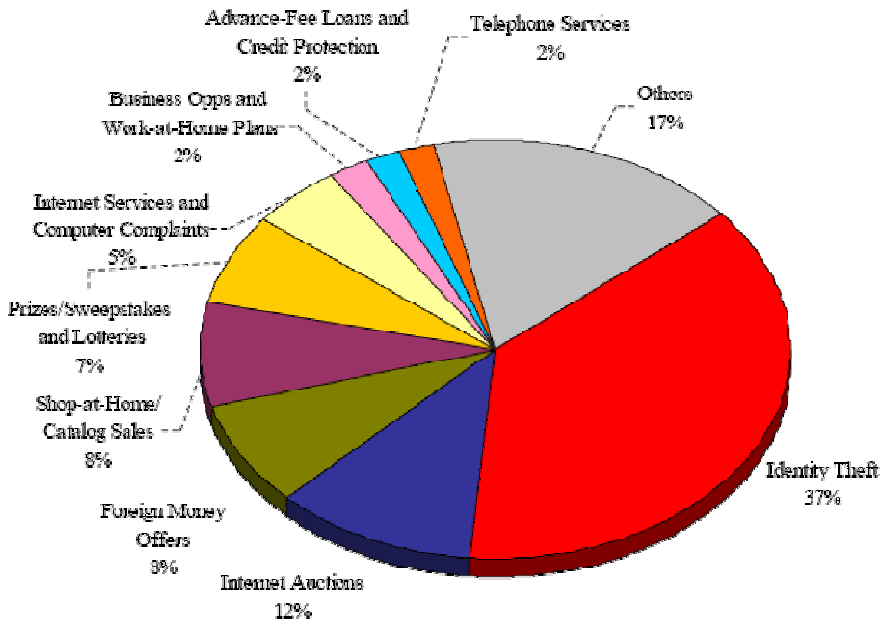
- 2006 Consumer Sentinel Survey
  - –657,591 complaints re: consumer fraud
  - –246,882 complaints re: ID Theft
  - –ID Theft the largest category of complaint (36%)
  - –48% of ID Theft activity is Internet related
    - •Internet auctions 5%
    - • Internet services 6%
  - –60% of consumers surveyed indicated that fraud was perpetrated through the Internet
    - •15% Websites
    - •45% Emails
  - –Total fraud reported was $1.1 billion; median loss $500.00

Available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf

More from the Federal Trade Commission

- Types of Fraudulent Activity
  - SSN not specifically compromised
    - Credit Card Theft 25%
  - SSN compromised
    - Phone and Utility Fraud 16%
    - Bank Fraud 16%
    - Employment Fraud 14%
    - Government Benefits 10%
    - Loans 5%

Sentinel Top Complaint Categories[1]
January 1 – December 31, 2005



Available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf

A Paradigm Shift

- For many regulated industries, the world changed in 1999. Ownership of consumer's personal information was "given back" to the consumer. It is now considered personal property, rather than a corporate asset. The organization may own the database, but they serve as the primary custodian of the personal information, rather than the owner. In effect, this extends the duty of care that many businesses and organizations owe to customers and consumers. They must now proactively protect personal information, in addition to providing goods or rendering services.

2005: Year of the Data Breach

Tufts University	PayMaxx	DOJ
Polo Ralph Lauren	Hinsdale High	Stanford Univ
CA FasTrack	Westborough Bank	Valdosta State
CA Dept of Health	Jackson CC	CardSystems
DSW Shoes	LexisNexis	Duke Univ
Ameritrade	U CA Berkeley	Cleveland State
Carnegie Mellon	Boston College	Merlin Data Services
Michigan State	Nevada DMV	Motorola
CSJ Hospital	Northwestern	CitiFinancial
Georgia Southern	UNLV	FDIC
Wachovia	Cal State Chico	MCI
Oklahoma State	U CA SF	SJ Medical
Time Warner	Georgia DMV	CO Dept of Health
ChoicePoint	Bank of America	Purdue Univ.
Air Force	University of Colorado	USC, Michigan, Southern California State
University of North Texas	Cisco.com	Sonoma State University

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

2006: The Good Times Just Keep Coming . . .

UPMC Squirrel Hill Family Medicine

H&R Block

Atlantis Hotel - Kerzner Int'l

People's Bank

City of San Diego, Water & Sewer Dept.
Univ. Place Conference Center & Hotel
Indiana Univ.

California Army National Guard

Univ. of Notre Dame

Univ. of WA Medical Center

Providence Home Services (OR)

State of RI web site

Boston Globe

The Worcester Telegram & Gazette

BCBS of North Carolina

FedEx

Honeywell International

Dept. of Agriculture

Old Dominion Univ.

BCBS of Florida

Calif. Dept. of Corrections, Pelican Bay

Mount St. Mary's Hospital (Lewiston, NY)

Deloitte & Touche (McAfee employee information)

Medco Health Solutions

OH Secretary of State's Office

Olympic Funding (Chicago, IL)

Los Angeles Cty. Dept. of Social Services Hamilton County Clerk of Courts

Metropolitan State College

Georgetown Univ.

Verizon Communications

iBill (Deerfield Beach, FL)

CA Dept. of Consumer Affairs

General Motors (Detroit, MI)

Buffalo Bisons and Choice One Online

Ernst & Young (UK)

Bananas.com

Fidelity Investments

CA State Employment Development Division Vermont State Colleges

Georgia Technology Authority
Conn. Technical High School System
Progressive Casualty Insurance

DiscountDomain
Registry.com

University of Medicine and Dentistry of New Jersey

Ross-Simons

Univ. of South Carolina

University of Alaska, Fairbanks

Ohio University Innovation Center University of Texas' McCombs School of Business

Univ. of Northern Iowa

Purdue University

Aetna -- health insurance records for employees of 2 members, including Omni Hotels and the Dept. of Defense NAF

MasterCard (Potentially UK only)

Long Island Rail Road
Ohio's Secretary of State

Dept. of Defense

Georgia State Government

Idaho Power Co.

Ohio University Hudson Health Center

Dept. of Veteran Affairs

Wells Fargo

Mercantile Potomac Bank
American Institute of Certified Public Accountants (AICPA)

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

2006: And Coming . . .

Univ. of Delaware

M&T Bank
Sacred Heart Univ.

American Red Cross, St. Louis Chapter

Vystar Credit Union

Texas Guaranteed Student Loan Corp.
Florida Int'l Univ.
Miami University

Univ. of Kentucky

Buckeye Community Health Plan

Ahold USA

YMCA

Humana

Internal Revenue Service

Univ. of Texas

Univ. of Michigan Credit Union

Denver Election Commission
U.S. Dept. of Energy

Minn. State Auditor
Oregon Dept. of Revenue
U.S. Dept of Energy, Hanford Nuclear Reservation
American Insurance Group (AIG)

NY State Controller's Office

ING
Univ. of Kentucky
Automatic Data Processing (ADP)

CA Dept. of Health Services (CDHS)

Equifax

Univ. of Alabama
U.S. Dept. of Agriculture (USDA)
Cape Fear Valley Health System
Fed. Trade Comm. (FTC)
San Francisco State Univ.
U.S. Navy
CA Dept. of Health Services (CDHS)
Catawba County Schools
King County Records, Elections, and Licensing Services Division
Gov't Accountability Office (GAO)
AAAAA Rent-A-Space
AllState Insurance Huntsville branch

Nebraska Treasurer's Office
Minnesota Dept. of Revenue
Nat'l Institutes of Health Federal Credit Union NIH

American Red Cross, Farmers Branch
Bisys Group Inc.
Automated Data Processing (ADP)

University of Tennessee
Nat'l Association of Securities Dealers (NASD)
Naval Safety Center

Montana Public Health and Human Services Dept.
Moraine Park Technical College

Northwestern Univ.
University of Iowa
Treasurer's computer in Circuit Court Clerk's office
Nelnet Inc.
CS Stars, subsidiary of insurance company
Marsh Inc.
U.S. Dept. of Agriculture
New York City Dept. of Homeless Services
Armstrong World Industries
Georgetown University Hospital
Old Mutual Capital Inc.

Cablevision systems

U. S. Navy recruitment offices

Kaiser Permanente Northern Calif. Office
Los Angeles County, Community Development Commission (CDC)
Los Angeles County, Adult Protective Services

Western Illinios Univ

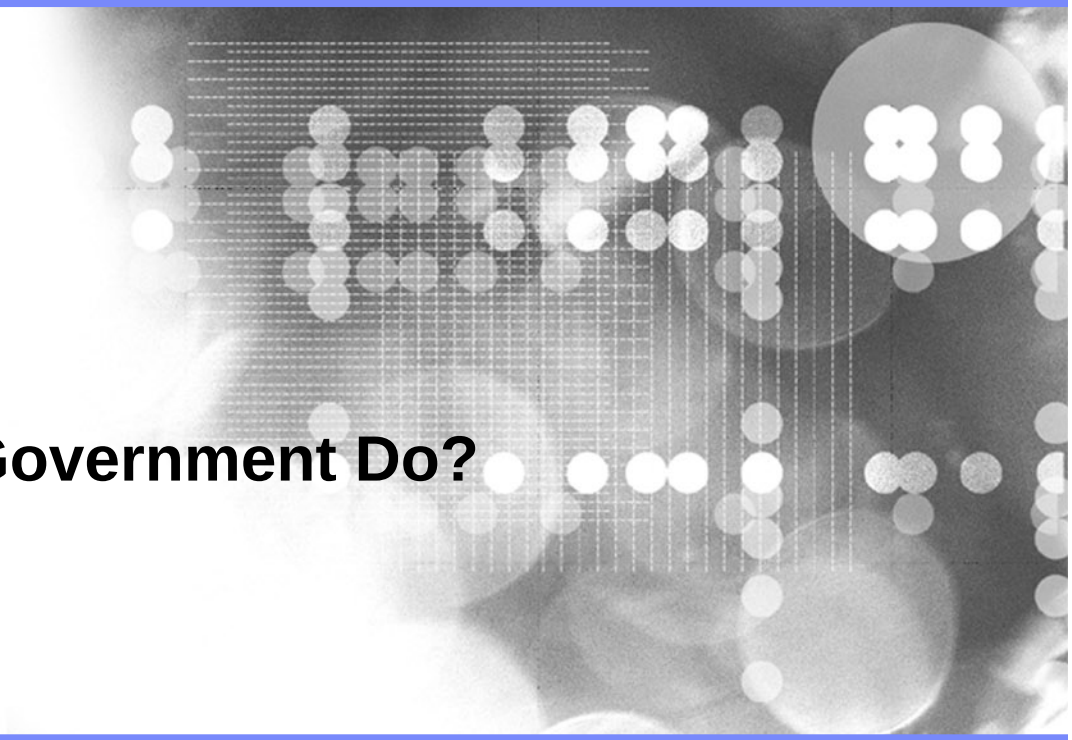
Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

2007: ???

- **January 2 – Deaconess Hospital – Evansville, IN**
- **January 4 – Unnamed medical center via recycling service – Stockton, CA**
- **January 5 – Dr. Baceski's Office – Somerset, PA**
- **January 25 – Ohio Board of Nursing – Columbus, OH**
- **January 26 – Anthem Blue Cross Blue Shield – VA**
- **February 2 – VA Medical Center – Birmingham, AL**
- **February 7 – Johns Hopkins University Hospital – Baltimore, MD**
- **February 8 – St. Mary's Hospital – Leonardtown, MD**
- **February 9 – Radford University, Waldron School of Health and Human Services – Radford, VA**
- **February 14 – Kaiser Medical Center – Oakland, CA**
- **February 19 – Seton Healthcare Network – North Austin, TX**
- **February 20 – Back and Joint Institute – San Antonio, TX**
- **Today or Tomorrow -- YOU ???**

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

IBM/Tivoli

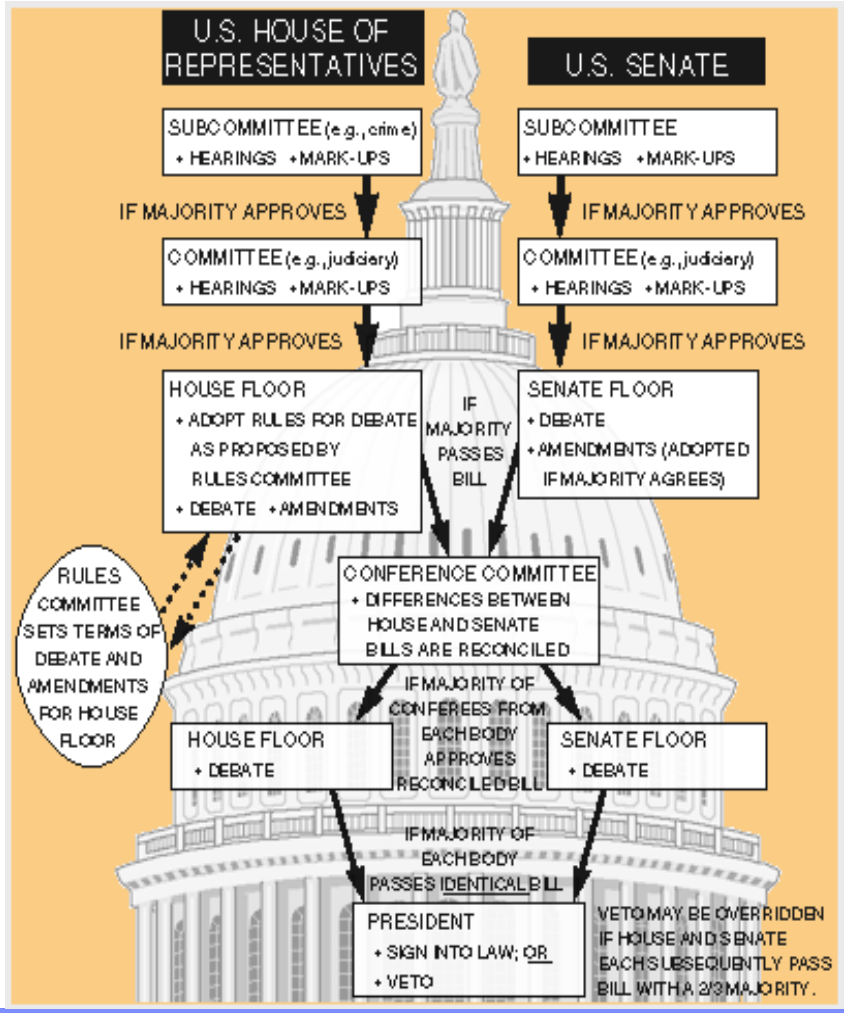


Notification Laws

What Can the Government Do?

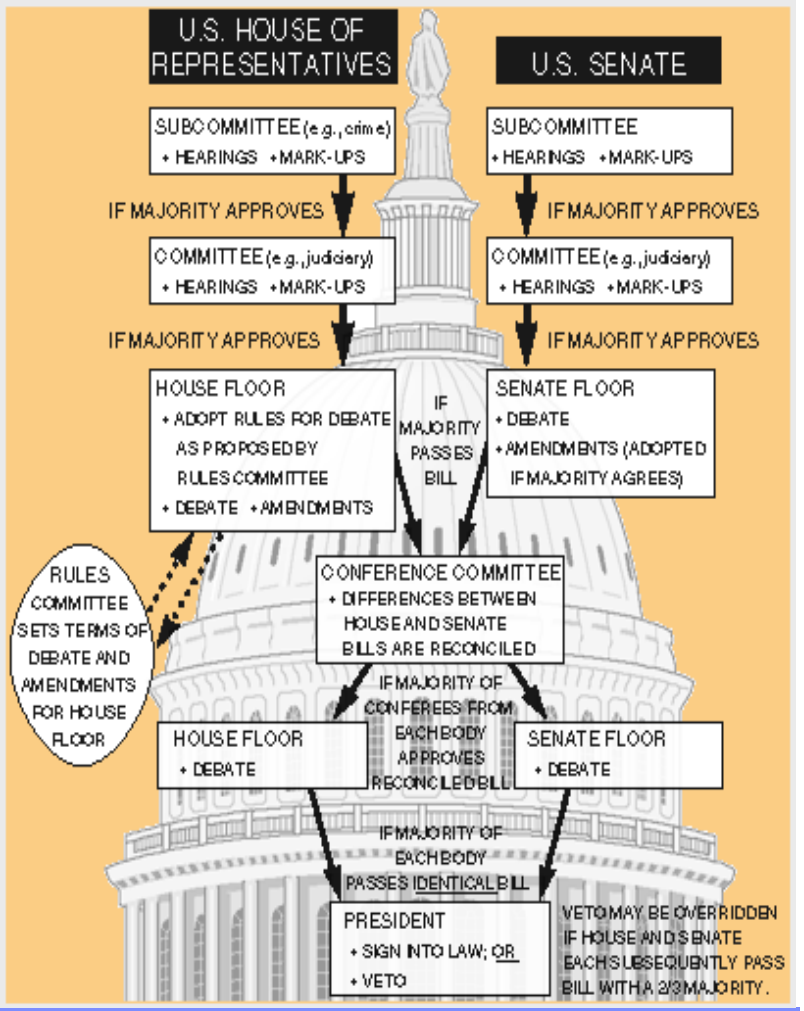
Federal Proposals – Dead in 2006

- **Identity Theft Protection Act (Introduced in Senate)**[S.1408.IS]
- **Consumer Data Security and Notification Act of 2005 (Introduced in House)**[H.R.3140.IH]
- **Notification of Risk to Personal Data Act (Introduced in House)**[H.R.1069.IH]
- **Notification of Risk to Personal Data Act (Introduced in Senate)**[S.115.IS]
- **Notification of Risk to Personal Data Act (Introduced in Senate)**[S.751.IS]
- **Consumer Notification and Financial Data Protection Act of 2005 (Introduced in House)**[H.R.3374.IH]
- **Notification of Risk to Personal Data Act (Introduced in Senate)**[S.1326.IS]
- **Personal Data Privacy and Security Act of 2005 (Placed on Calendar in Senate)**[S.1332.PCS]
- **Personal Data Privacy and Security Act of 2005 (Reported in Senate)**[S.1789.RS]



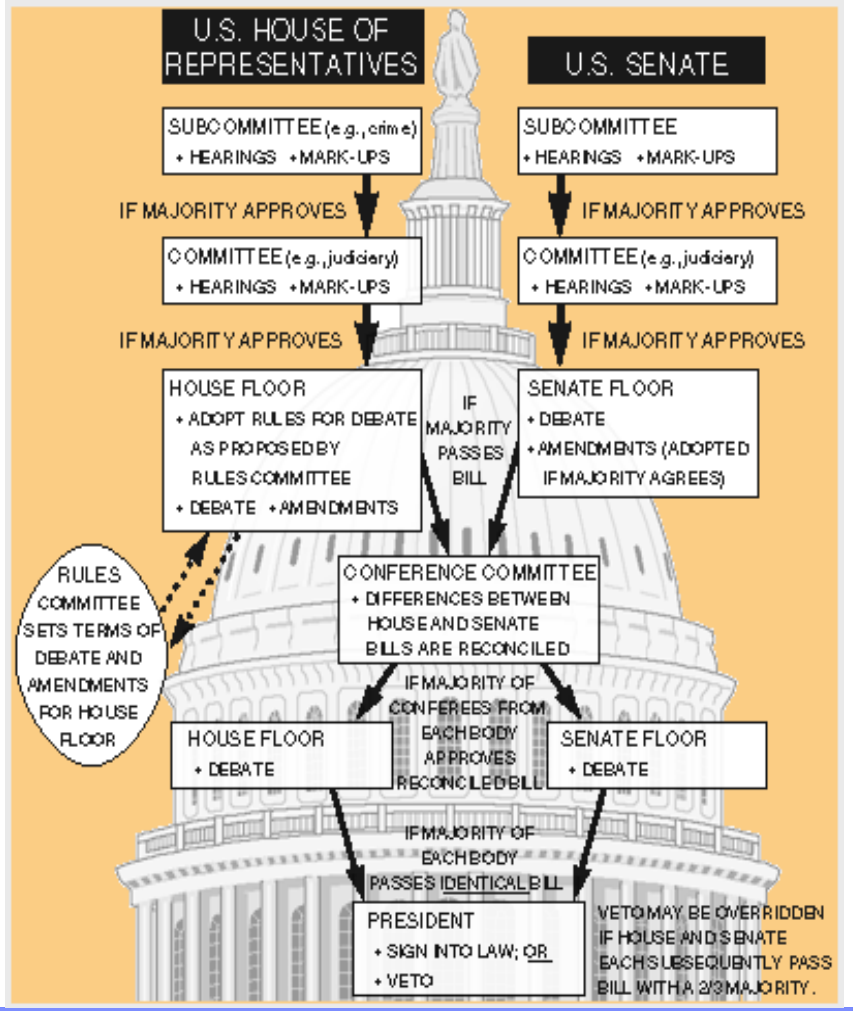
Federal Proposals – New in 2007

- **Data Accountability and Trust Act (Introduced in House)[H.R.958.IH]**
- **Cyber-Security Enhancement and Consumer Data Protection Act of 2007 (Introduced in House)[H.R.836.IH]**
- **Notification of Risk to Personal Data Act of 2007 (Introduced in Senate)[S.239.IS]**
- **5 . VIP Act (Introduced in House)[H.R.1307.IH] (applies to victims of the 2006 VA breach only)**
- **Prevention of Fraudulent Access to Phone Records Act (Introduced in House)[H.R.936.IH]**



Leahy-Specter

- **Leahy-Specter Personal Data Privacy and Security Act of 2007 (Introduced February 2007 in the Senate)** [S.495.IS]
- **Summary**
  - General: Provides Americans with notice when they have been harmed, and also addresses the underlying problem of lax security and lack of accountability in dealing with personal data.
  - Adds unauthorized access to sensitive personally identifiable information to the criminal prohibition against computer fraud under 18 U.S.C. § 1030(a)(2).
  - Requires data brokers to let individuals know what information they have about them, and where appropriate, allow individuals to correct demonstrated inaccuracies. Exemptions for:
    - products and services subject to the Fair Credit Reporting Act
    - Gramm-Leach-Bliley and the Health Information Portability and Accountability Act.
    - proprietary, fraud prevention tools and marketing data.
  - 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.



Leahy-Specter (con't.)

- **Leahy-Specter Personal Data Privacy and Security Act of 2007 (Introduced February 2007 in the Senate)** [S.495.IS]
- **Summary (con't.)**
  - Requires notice to law enforcement, consumers and credit reporting agencies when digitized sensitive personal information has been compromised. The trigger is tied to significant risk of harm with appropriate checks-and-balances to prevent over-notification or underreporting. Exemptions for
    - national security and law enforcement needs
    - credit card companies using fraud-prevention techniques
    - where a breach does not result in a significant risk of harm.
  - Addresses the government's use of personal data by:
    - (1) General Services Administration evaluates privacy and security practices of potential government contractors handling personal data (penalties in government contracts for failure to protect data);
    - (2) Federal departments and agencies audit infosec practices of commercial data brokers for projects involving personal data (protections and penalties in contracts with data brokers to protect data); and
    - (3) Federal departments and agencies conduct privacy impact assessments on commercial databases containing personal data on U.S. persons, and adopt regulations to ensure the security and privacy of data obtained through commercial data brokers.
  - Imposes a criminal penalty in the cases were there is intentional and willful concealment of a security breach known to require notice.

Federal Proposals – Who must comply

Bill	H.R. 836	S.239	H.R.958
Who?	**"Consumer Reporter" Consumer reporting agencies, retailers, holders of sensitive financial account info**	**Any "covered" entity. FTC Determines information covered**	**Any business entity that collects sensitive info on 10,000 or more people**

Federal Proposals - Notice Trigger

Trigger	H.R. 836	S.239	H.R. 958
Give notice when . . .	**It is reasonably likely that sensitive financial identity and account info will be used to commit fraud that will cause substantial harm**	**It creates a reasonable risk of identity theft**	**Sensitive personally identifiable info was subject to the breach**

Federal Proposals – Enforcement & Preemption

	H.R. 836	S.239	H.R. 958
Enforcement	**No Private Right of Action**	**Split by Agency** **FTC, State AG** **NPRA**	**USAG** **NPRA**
Preemption	**Preempts**	**Preempts**	**Preempts**

Federal Regulation

- ***Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 70 Fed. Reg. 15736 (3/29/05)**
- **Applies to retail financial institutions (includes offshore entities) *and their service providers***
- **Issued as supplemental guidance to the Financial Services Modernization Act of 1999 (a.k.a. Gramm-Leach-Bliley)**
- **Defines "sensitive customer information" more broadly than state laws.**
- **Places burden to act responsibly on the banks, thrifts and credit unions.**

Notification Now Tied Directly to Incident Response

- **Suspect unauthorized individuals have gained access to customer information.**
- **Identify affected customer information systems and types of customer information.**
- **Conclude that incident (i) actually does involve unauthorized access and (ii) involves sensitive customer information.**
- **Notify federal regulator and begin an investigation of the likelihood that such information has been or will be misused.**
- **Notify "appropriate law enforcement authorities" and file a suspicious activity report (SAR).**
- **Take steps to contain and control the incident.**
- **If it is "reasonably possible" that sensitive customer information will be misused, notify each affected customer.**
- **Delay customer notification if requested, in writing, by a law enforcement authority to avoid compromising a criminal investigation.**

35 State Laws So Far . . .

ARKANSAS **(SB 1167)**	ILLINOIS **(H.B. 1633)**	NEW HAMPSHIRE **(RSA 359-C:20)**
ARIZONA **(SB 1338)**	INDIANA **(SB 503)**	NEW JERSEY(A4001)
CALIFORNIA **(SB 1386)**	KANSAS **(SB196)**	NEW YORK **(4254-A)**
COLORADO **(HB1119)**	LOUISIANA **(SB 205)**	NORTH CAROLINA **(SB 1048)**
CONNECTICUT **(SB 650)**	MAINE **(LD 1671)**	NORTH DAKOTA **(SB 2251)**
DELAWARE **(HB 116)**	MICHIGAN **(SB 309)**	OHIO **(HB 104)**
FLORIDA **(HB 481)**	MINNESOTA **(HF 2121) [Businesses]** **(HF 225) [Government Agencies]**	OKLAHOMA **(74.49.3113.1)**
GEORGIA **(SB 230)**	MONTANA **(HB 732):**	PENNSYLVANIA **(SB 712)**
HAWAII **(SB2290)**	NEBRSKA **(LB 876 [Section 87-803])**	RHODE ISLAND **(H 6191)**
IDAHO **(Title 28-51)**	NEVADA **(SB 347) [Businesses] (AB 334) [Government Agencies]**	TENNESSEE **(SB 2220)** TEXAS **(SB 122)** UTAH **(13-44-202)** VERMONT **(9-62 §2435)** WASHINGTON **(SB 6043)** WISCONSIN **(895.507)**

Pending and Trending . . . .

- ***Security breach bills pending****:* CA (updated version), MA, PA (updated version)
- ***Bills under consideration****:* MD, MO, OR, SC, VA, WV
- ***No laws***: AL, AK, IA, KY, MS, NM, SD, WY, DC

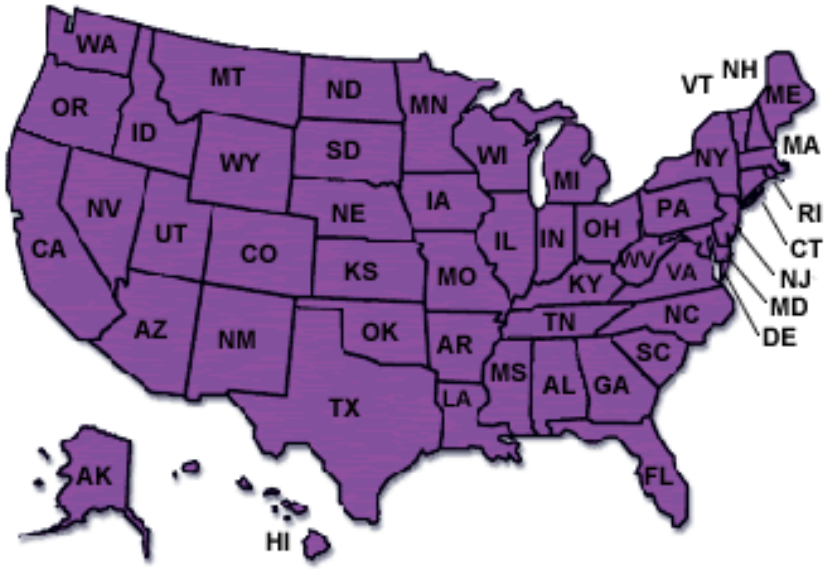
- **Exceptions in the 2006 Laws**:
- **AZ** – does not apply to HIPAA and GLB affected organizations; does not allow encryption exemption
- **CO** – organizations subject to Federal notification mandates are deemed already in compliance with the state statute
- **HI** – HIPAA and GLB affected organizations are deemed in compliance; no private right of action, but the attorney general may bring a civil suit; fines are capped at $2500 per incident; government agencies are exempt from prosecution
- **ID** – allows for private right of action; mandates payment card account number truncation on merchant receipts
- **KS** – organizations subject to Federal notification mandates are deemed already in compliance with the state statute
- **NH** – GLB exception

Source: http://www.pirg.org/consumer/credit/statelaws.htm

- **WI** – allows for private right of action; all regulated entities exempt

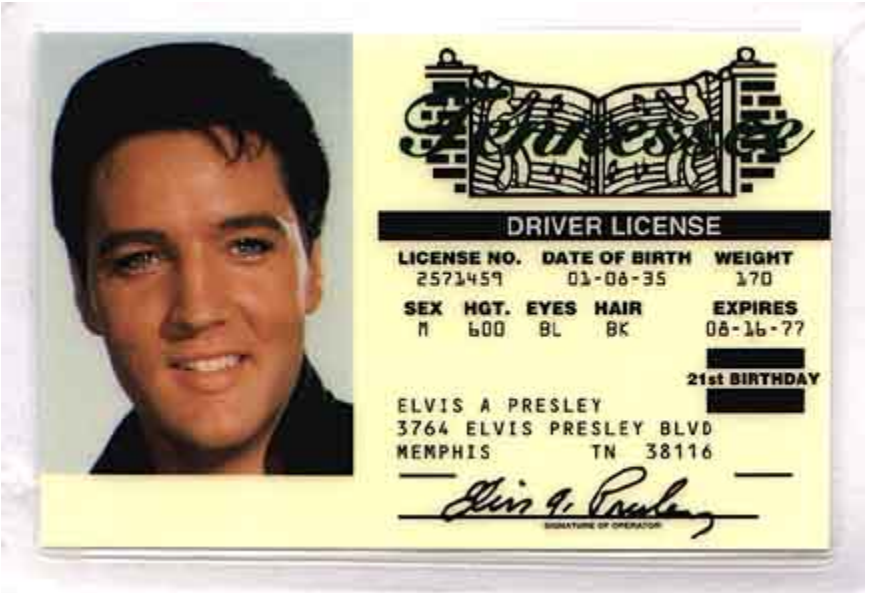
State Laws (in general)

- **Breaches of unencrypted *personal information***
- **Must affect 1,000 or more individuals**
- **The organization must determine if misuse of the information is likely**
- **Written notification after a breach is discovered**
- **Substitute notice via announcements**
- **Delay notice for law enforcement investigation**
- **State attorneys general have enforcement authority**
- **No private right of action**
- **Government agencies exempt from civil action**



“Personal Information”

- **Arkansas, Delaware – includes medical information**
- **Georgia – Includes password alone if it would allow access to data identifying data subject by name**
- **North Dakota - includes date of birth, mother's maiden name, employer ID, e-signature, and birth, death, or marriage certificate.**
- **Indiana - “breach” does not include loss of a “portable electronic device”**



Who Must Comply

- **Texas, North Dakota, Montana – applies only to business**
- **Indiana, Oklahoma – applies only to government agencies**
- **Georgia, Maine – applies only to data brokers**

Legal Threshold - Notice Not Required If:

- **Arkansas, Louisiana**
  - "no reasonable likelihood of harm to customers."
- **Connecticut**
  - law enforcement investigation concludes breach "will not likely result in harm."
- **Rhode Island**
  - law enforcement finds no "significant risk of identity theft."
- **Delaware**
  - covered entity's investigation finds no reasonable likelihood that breached data has or will be "misused."
- **Florida**
  - covered entity finds harm unlikely.
- **California**
  - all "unauthorized access."
- **Common law liability approach**

IBM/Tivoli

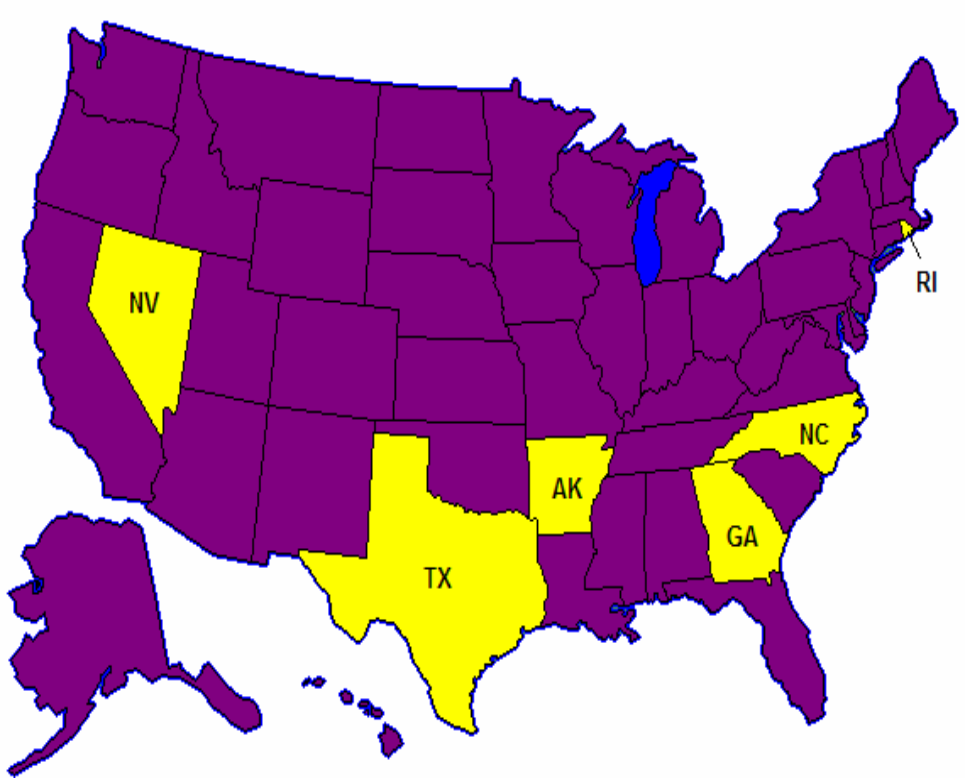
InfoSec and the Myth of Encryption

Template DocumentationHIPAA
Summit XIV
Session 10.04

3/26/2007March
2007

What's Missing from State Law ??

- Out of the 35 laws on the books, only 6 states require the organization to have an information security program in place.
- Essentially, we are conceding that a breach is inevitable.
- Making the only duty of care the organization owes to the consumer that of notification rather than protection.
- D'Oh !!!



Focus on Destruction

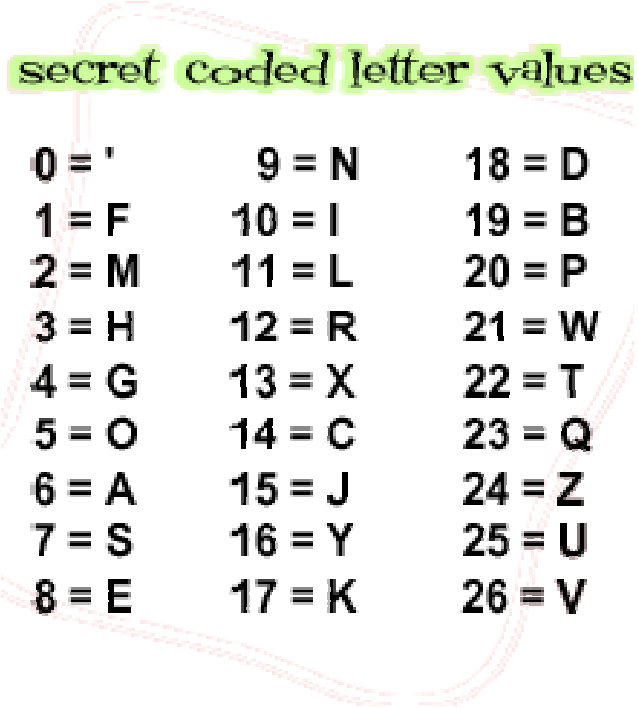
- **NV State Law**
  - **Senate Bill No. 347–Senators Wiener, Titus, Raggio and Townsend**
  - **Joint Sponsor: Assemblyman Anderson**
- CHAPTER.....
- Sec. 22. *1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.*
- *2. As used in this section:*
- *(a) "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.*
- *(b) "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:*
- *(1) Shredding of the record containing the personal information; or*
- *(2) Erasing of the personal information from the records.*

Reliance on Other Laws and Regulations

- **NV State Law (con't)**
- Sec. 23. *1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.*
- *2. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.*
- *3. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.*

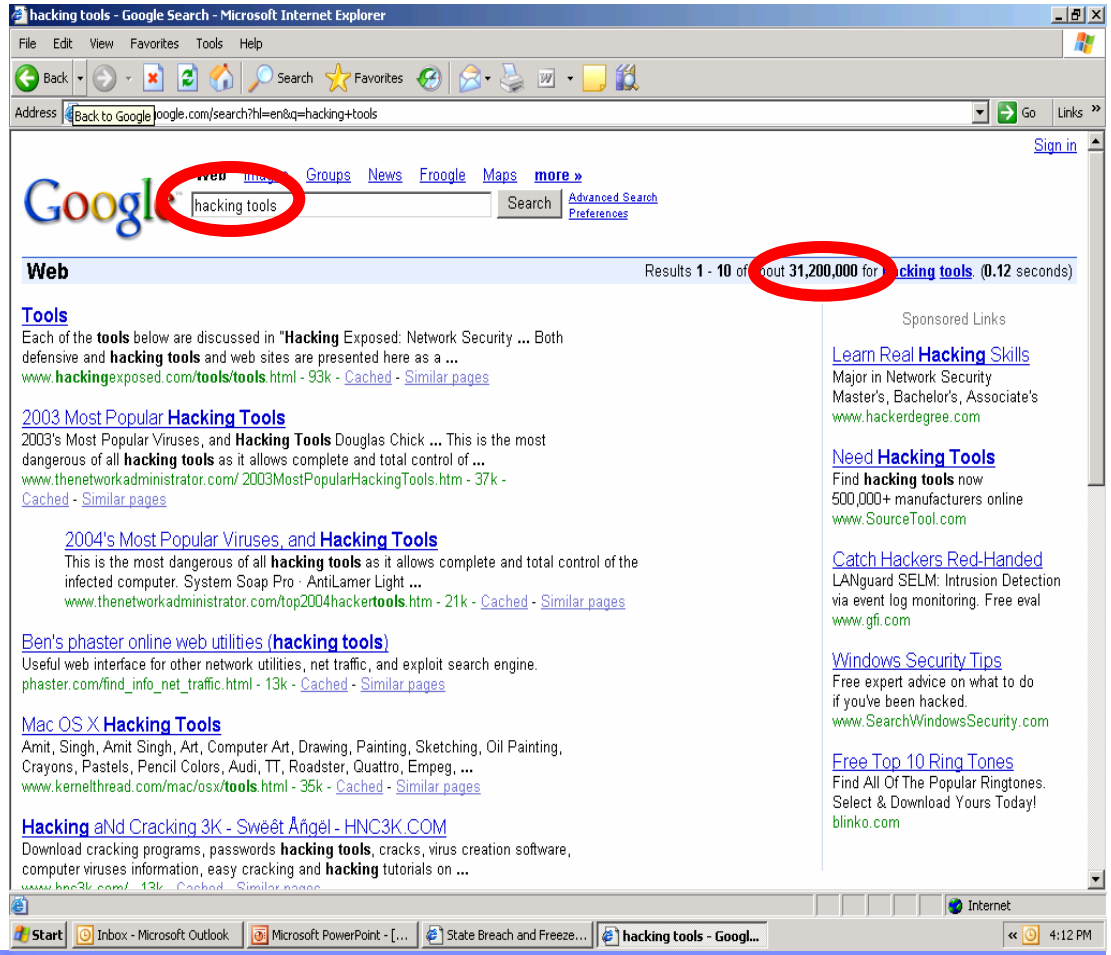
Instead, We Rely On Two Protections

- Redaction – the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data (new trend in 2006)
- Many States Exempt Notice Requirements if the Data is ***Stored in an Encrypted Format***
- Industry best practices promulgate the idea that encrypted data cannot be easily compromised
- Real life, however, indicates that data encryption provides no real protection at the point of attack
- **Are you relying on data encryption as a silver bullet???**



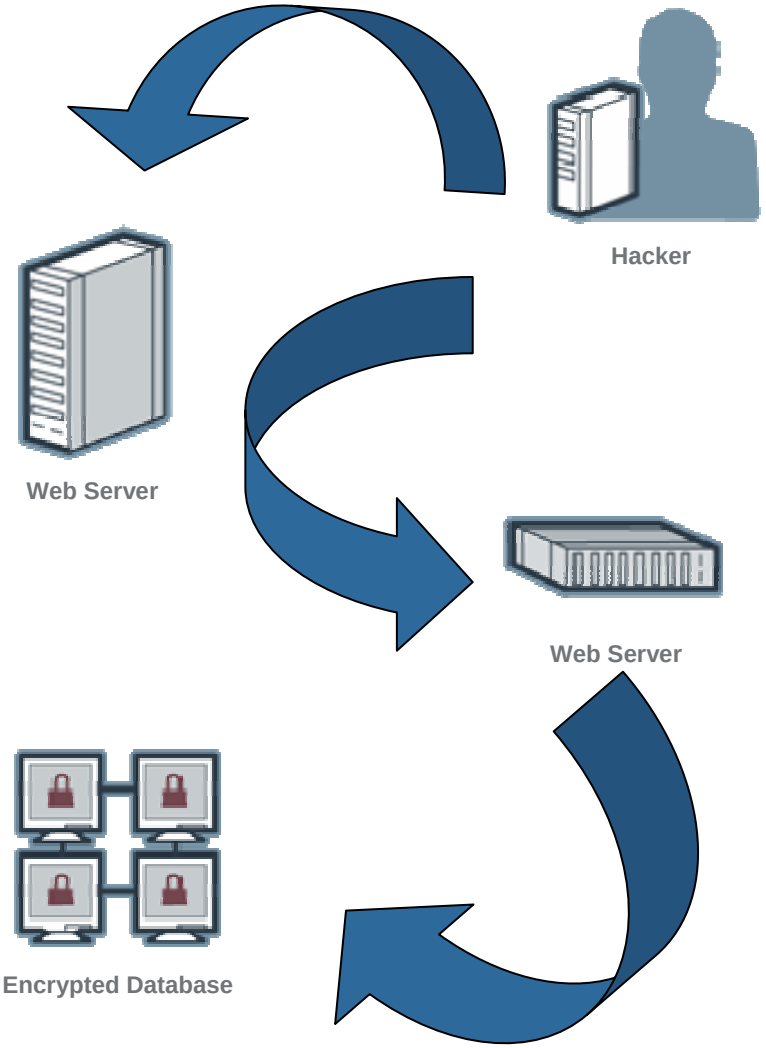
Common Attacks

- Attacks on databases are the most lucrative
- Hackers gain access to thousands of pieces of personal data through a single compromise
- The most effective compromises exploit basic functionality that makes data available to legitimate users
- Electronic hacking tools are freely available on the web



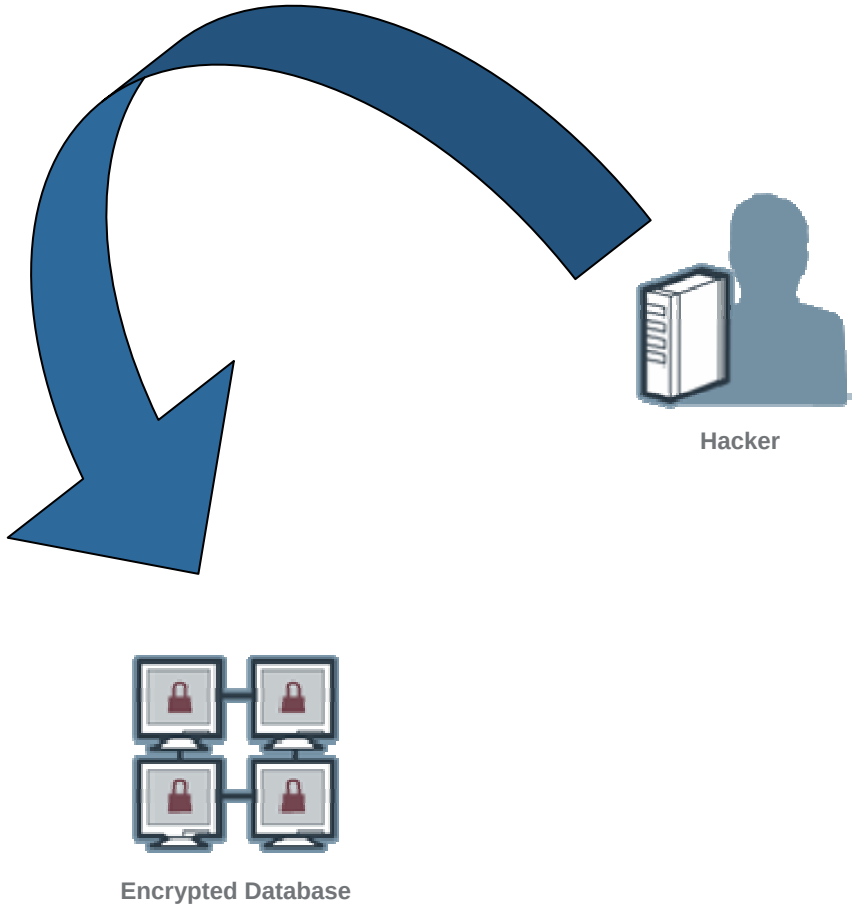
Web Server Hack

- Scenario: Hacker compromises a web server. Root compromise of the server allows the hacker to make database calls using the credentials of an administrators. Database serves up data unencrypted, because the call is made from the correct web server.



Database Hack

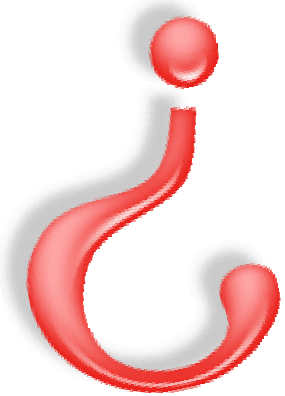
- Scenario: Hacker directly compromises an SQL database. Root compromise of the server allows the hacker to access data using the credentials of a DBA. Database serves up data unencrypted, because the call is made from the correct “super” user.

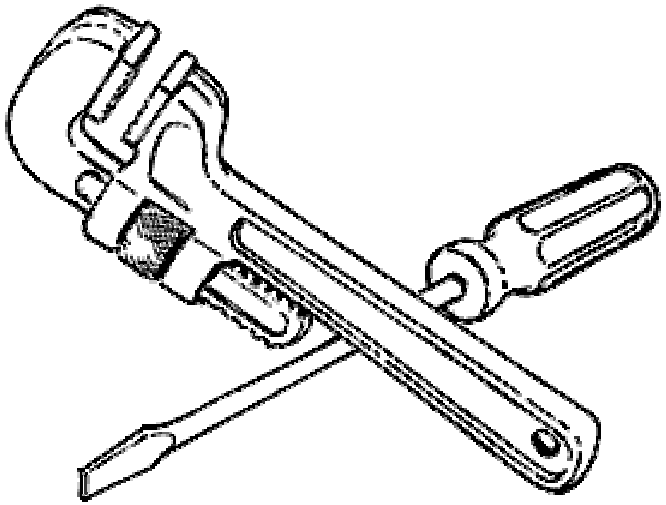


Physical Attack

- Scenario: Thief physically steals a database server. Database is encrypted but crypto keys are stored on that server. While the drive is up and running, the data is unencrypted. Once the power is cut, however, the database encrypts.

Fix, Prosecute or Notify??





When to Notify ??

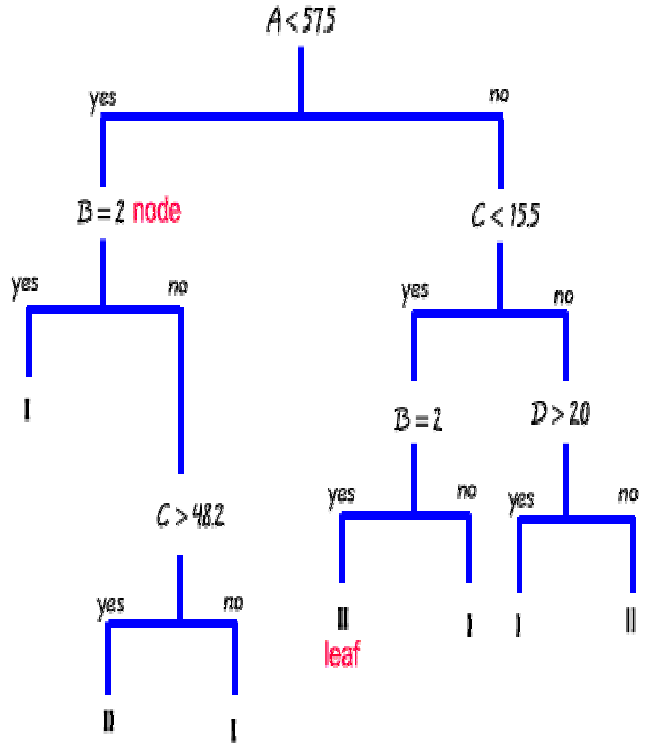
- What do the laws really require in terms of encryption
  - **CA SB 1386**
    - Carves out an exemption if the data is encrypted in storage.
  - **Common interpretation**
    - As long as the organization encrypts data in storage, they do not have to notify
  - **But, ask yourself**
    - Was the data in storage at the time of the attack ??
      - Example 1 – Web Server Hack ?
      - Example 2 – Database Hack ?
      - Example 3 – Physical Attack ?
  - **Rule of thumb for encryption**
    - **In all cases of breach, notify, unless there is evidence to suggest reasonable assurance that the data was encrypted at the point of attack.**
    - **Look for the courts to establish this as precedent**

When to Fix ??

- Resolution of incidents is at the discretion of the organization
  - **Typically, fixing is associated with simple mistakes**
    - Blunders
    - Misuse of privilege
    - Well-intentioned employees
  - **Administrative matters**
    - No evidence of criminal intent
    - No harm done
    - May involve disciplinary measures for the employee
    - Formal documentation of the incident is sufficient
  - **Notify ??**
    - Look to specifics of state law

Investigative Response

- Neither Federal regulation nor state law currently require investigation or prosecution
  - **Not a decision that the organization can reasonably make during an incident**
  - **Create a decision tree**
    - Establish parameters – when to fix, if and when to investigate
    - Fixing and investigating can sometimes be mutually exclusive
    - Organization needs to understand the impact of investigation and prosecution
    - Incorporate these decisions and procedures into the Incident Response Plan



When to Prosecute ??

- Also at the discretion of the organization
  - **Typically associated with complex attacks**
    - Malicious intent
  - **Civil or criminal activity**
    - Sensitive data clearly accessed, stolen, altered
    - Damage to systems, services, devices, or data
    - Evidence of an external intruder
  - **Furtherance of the organization's good faith effort**
    - Hard to prove negligence
    - Satisfies common law liability

Brace for Impact

- In either case, the organization must be prepared
  - **Freeze systems as long as it takes to establish the forensic trail**
    - Isolate affected systems
    - Invoke business continuity plan to maintain operations
  - **Submit to the authorities**
    - Local law enforcement search
    - Federal law enforcement search and seizure of equipment and data
    - Provide resources for the duration of the investigation
  - **Prosecution takes time and resources**
  - **In cases of organized crime, revenge is an issue**
    - Be prepared for retaliatory attacks on systems and data
  - **Investigation and prosecution may delay notification**

But this is all after the fact

- **Affected organizations should set up a security program to mitigate risk, and protect from breaches to the extent reasonably possible**
- **At minimum**
  - Identify systems containing personal information and improve intrusion detection.
  - Encrypt personal information. (maybe)
  - Ensure that third-party contracts involving the transfer of personal data include information security provisions.

A Sound Information Security Program

Reviews HR & Management Issues

- Hiring and retention policies for IT/security staff & end-users
- Adequate staffing, authority, responsibility, succession
- "Key Man" and training policies
- Termination

"Institutionalize" InfoSec

- IT in Corporate Governance
- Management Philosophy
- Corporate Culture
- Periodic training and review for all personnel

Reviews Network Architecture

- Segmentation
- Critical Devices
- User rights and permission

Inspects Physical Security

- Door locks and alarms
- Security cameras and monitoring
- Visitor access logs
- HVAC, fire suppression, etc.
- Racks and cabling

Reviews Business Policies & Procedures

- Backup and failover contingency
- Redundancy, disaster recovery, and business continuity planning
- Current equipment inventory
- Third-party provider SLAs & liability
- User rights and permissions
- End-user computing policies

Performs electronic testing

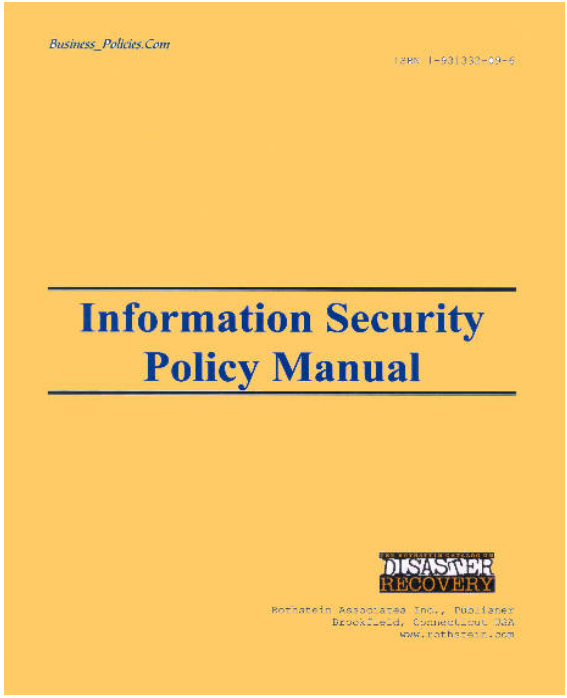
- Firewall(s) & Routers
- Devices visible to the Internet
- Network segmentation
- Active/Inactive modems
- OS levels & patches
- Anti-virus software

That being said

- **Accept that there are no 100% guarantees with information security**
- **Establish a level of risk tolerance based upon a thorough, document risk assessment**
- **Make notification a part of your incident response plan and your disaster recovery plan**

Policy Changes

- **Write a corporate incident response policy that includes notification.**
- **Incident response plan should**
  - Require immidiate notification of key decision-makers upon detection of a loss or breach.
  - Include a statement regarding investigative procedures in the event of a security breach.
  - Include a statement regarding organized, coherent communication with the public regarding security measures.



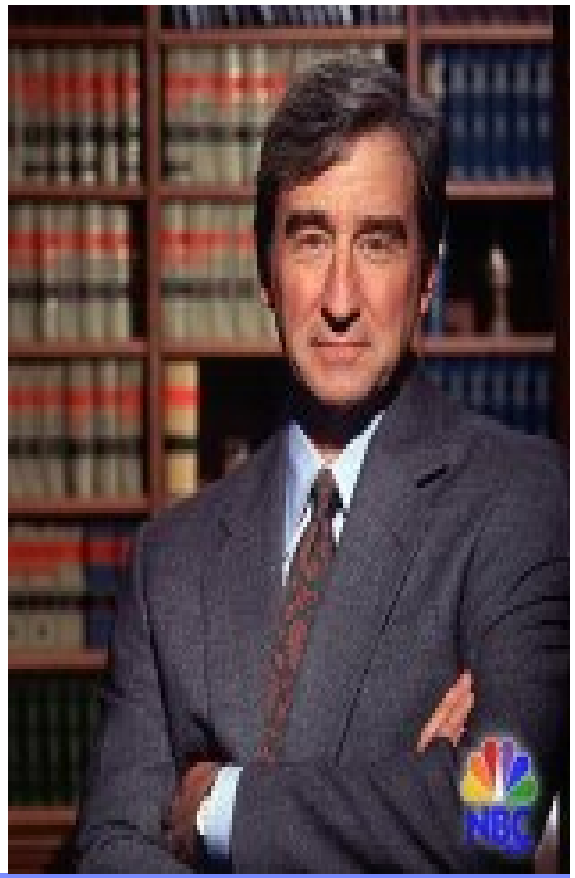
Collateral Issues to Consider

- Extend IR Plan across the enterprise
- Just like the organization's security program, the IR Plan must become part of the corporate culture
- Incident Response Plan must be supported in-house
- Include HR, PR, Legal, Administration, and Senior Management

Summing Up . . .

Lawyer up !!

- **In the event of a security breach**
  - Know when to notify
  - Do the extrapolated thinking
  - Make notification a part of the incident response plan
  - Offer assistance to the affected individuals when appropriate
- **But most importantly**
  - have an efficient infosec program in place to mitigate against breaches
- **Compliance means never having to say you're sorry…..**



Questions? Comments? More Info?

- **GRC Information –** www.ibm.com/servicessolutions/us
  - **Education and Training**
  - **Services by Industry**
  - **Services by Business Issue**

- **Contact Info**

Marne E. Gordan

GRC Market Manager

mgordan@us.ibm.com

703/960-9536