

**Effective, Continuous Compliance:
HIPAA, PCI-DSS, RED FLAG**
prepared for: ISC2 eSymposium, Aug17 2010

Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
raj@brainlink.com / 917-685-7731

Raj Goel, CISSP

Raj Goel, CISSP, is an Oracle and Solaris expert and he has over 20 years of experience in software development, systems, networks, communications and security for the financial, banking, insurance, health care and pharmaceutical industries. Raj is a regular speaker on HIPAA, Sarbanes-Oxley, PCI-DSS Credit Card Security, Information Security and other technology and business issues, addressing diverse audiences including technologists, policy-makers, front-line workers and corporate executives.

He also works with community and professional organizations such as the InfraGard, ISC2, and TibetAid.org, Association of Cancer Online Research - ACOR.org.



A nationally known expert, Raj has appeared in over 20 magazine and newspaper articles worldwide, including **Entrepreneur Magazine**, **Business2.0** and **InformationWeek**, and on television including **CNNfn** and **Geraldo At Large**.

Agenda

- Summary of Breaches
- HIPAA
- PCI
- RED FLAG
- Case Studies

2005 – 2009 summary

| | | |
|--------------------------------|--------------------|-----|
| <i>hacker</i> | <u>256,044,318</u> | * |
| <i>stolen computer</i> | <u>100,865,672</u> | |
| <i>insider</i> | <u>31,039,442</u> | |
| <i>tape lost</i> | <u>20,735,379</u> | |
| <i>unsanitary web practice</i> | <u>11,987,329</u> | |
| <i>poor process</i> | <u>6,378,201</u> | |
| <i>unshredded paper</i> | <u>2,270,247</u> | |
| <i>hd stolen</i> | <u>723,200</u> | |
| <i>social engineering</i> | <u>714,000</u> | ** |
| <i>crimeware</i> | <u>197,000</u> | *** |
| <i>unsanitized drives</i> | <u>113,183</u> | |
| <i>briefcase stolen</i> | <u>41,460</u> | |
| Total | 431,109,431 | |

* Is it really hacking, or dishonest insiders or poor processes?

** Data collection firms allowed criminals to setup customer accounts and sold them data

*** A custom virus against a university,
and unknown how many PCs were
infected via
Google Ads serving malware

What's HIPAA?

Health Insurance Portability and Accountability Act of 1996

3 Sections

- Privacy
- Transactions Code Sets
- Security

Goals:

- Reduce Administrative overhead costs (\$0.26)
- Reduce Fraud & Abuse (\$0.11)
- Protect privacy

HIPAA Penalties

- \$ 100 - \$25,000/person for a single standard in a year per violation
- Knowing misusing PHI up to \$ 50,000 and/or 1 year in prison
- Misuse under false pretenses up to \$ 100,000 and/or 5 years in prison
- Misuse with intent to sell or use for commercial gain \$ 250,000 and/or up to 10 years in prison
- BAD PUBLICITY

Protected Fields

- Names
 - Postal address
 - Tel & fax number
 - Email address
 - SSN
 - Medical record number
 - Health plan number
 - Certificate/license number
 - Vehicle ID or license
 - Device identifiers
 - Web URLs
 - Internet protocol
 - Biometric ID
 - Full face, comparable image
- Latanya Sweeney showed that 87% of all Americans can be identified by ZIP Code, DOB, sex.

Real world challenges

"For many 1-person medical offices, the CIO is somebody's child down the road who's really good at Nintendo."

- Howard Schmidt, US CyberSecurity CZAR

HITECH Changes to HIPAA

Implement
“meaningful
use” EHRs
and get
Federal
Grants



Greater
Penalties

Larger
Scope

Closed
Loopholes

HITECH Changes to HIPAA

1. Increased Penalties (willful neglect penalties have no limit!)
2. Secretary of HHS is required to fully investigate if initial complaint indicates possible willful neglect* (ignorance is no longer a defence)
3. State AGs may also sue HIPAA violators
4. HIPAA provisions directly apply to Business Associates
5. Notify customers, HHS, Media within 60 days
6. Lose > 500 records, join HHS' Hall Of Shame!

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>

FTC Health Breach Rule

FTC: Organizations not bound by HIPAA must report breaches

- *Web based businesses that deal with personal health information, even if they are not bound by HIPAA laws, to report security breaches.*
 - Shot across the bow to Google Health, MS Health, etc.
- The Health Breach Notification Rule created as a result of the American Recovery and Reinvestment Act (ARRA) of 2009.
- If a service provider breaches, they must notify the covered entity, who must notify customers.

NOTE: “UNSECURED PHI” == “Unencrypted PHI”

FTC Health Breach Rule

Differentiates between “unauthorized access” and “acquisition”

(1) the employee viewed the records to find health information about a particular public figure and sold the information to a national gossip magazine;

(2) the employee viewed the records to obtain information about his or her friends;

(3) the employee inadvertently accessed the database, realized that it was not the one he or she intended to view, and logged off without reading, using, or disclosing anything.

FTC Health Breach Rule

“If an entity’s employee loses a laptop containing unsecured health information in a public place, the information would be accessible to unauthorized persons, giving rise to a presumption that unauthorized acquisition has occurred. The entity can rebut this presumption by showing that the laptop was recovered, and that forensic analysis revealed that files were never opened, altered, transferred, or otherwise compromised. “

“Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information”

FTC Health Breach Rule

PHR related entities include non-HIPAA covered entities “that access information in a personal health record or send information to a personal health record.”

This category could include online applications through which individuals, for example, connect their blood pressure cuffs, blood glucose monitors, or other devices so that the results could be tracked through their personal health records. It could also include an online medication or weight tracking program that pulls information from a personal health record.

FTC Health Breach Rule

PHR identifiable health information =

1) *“past, present, or future payment for the provision of health care to an individual,”*

e.g. database containing names and credit card information, even if no other information was included

FTC Health Breach Rule

2) *“the fact of having an account with a vendor of personal health records or related entity,”*

e.g. the theft of an unsecured customer list of a vendor of personal health records or related entity

directed to AIDS patients or people with mental illness would require a breach

notification, even if no specific health information is contained in that list.

PCI-DSS – 12 Basic Requirements

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

PCI-DSS Penalties

1

Restrictions on the merchant or

2

Permanent prohibition of the merchant or service provider's participation in Visa programs.

3

In addition, the following fines apply for non-compliance, within a rolling 12-month period:

- First Violation - \$50,000
- Second Violation - \$100,000
- Third Violation - Management Discretion
 - Permanently prohibit the merchant or its agent from participating in Visa programs

Real world challenges

- Banks are “rebating” penalties, absorbing penalties or spreading penalties to all merchants
- HIPAA & SOX security requirements map neatly. PCI-DSS requirements could induce false sense of security.

Real world challenges

- No real teeth – most large offenders are still in business.
- VISA's "Verified By VISA" program violates PCI rules
- Rule enforcement is opaque and seemingly arbitrary.

FTC's RED FLAG Rules

What are the “red flags”?

Warning signs that ID theft may, or has, occurred.

“Financial Institutions” and “Creditors” must develop and implement written ID theft prevention programs that:

- 1. Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;*
- 2. Detect Red Flags that have been incorporated into its program;*
- 3. Respond appropriately to any Red Flags that are detected;*
- 4. Update the program periodically to reflect changes in risks from identity theft to customers and to the safety and soundness of the creditor from identity theft.*

FTC's RED FLAG Rules

- This is GLBA for Attorneys, Doctors, Hospitals, Small Businesses, etc.
- AMA, ABA and others have sued to exempt their members
- Currently excludes businesses with less than 20 employees
- Compliance extended 5 times – currently, not till Dec 2010

FTC & DSW

“Shoe retailer DSW Inc. agreed to beef up its computer security to settle U.S. charges that it **didn't adequately protect customers' credit cards and checking accounts**,...

The FTC said the company **engaged in an unfair business practice** because it created unnecessary risks by **storing customer information in an unencrypted manner without adequate protection**....

As part of the settlement, **DSW** set up a comprehensive data-security program and **will undergo audits every two years for the next 20 years.** “

- ComputerWorld.com 12/1/2005

According to DSW's SEC filings, as of July 2005, the **company's exposure for losses** related to the breach ranges **from \$6.5 million to \$9.5 million.**

This is the FTC's seventh case challenging faulty data security practices by retailers and others. - www.ftc.gov 12/1/2005

FTC & Choicepoint

“The **\$10 million fine** imposed today by the Federal Trade Commission on data aggregator ChoicePoint Inc. for a data security breach is yet another indication of the increasingly tough stance the agency is taking on companies that fail to adequately protect sensitive data, legal experts said.

And it's not just companies that suffer data breaches that should be concerned. **Those companies that are unable to demonstrate due diligence when it comes to information security practices could also wind up in the FTC's crosshairs**, they added.

- ChoicePoint will pay a fine of \$10 million...
- In addition to the penalty, the largest ever levied by the FTC, ChoicePoint has been asked to **set up a \$5 million trust fund for individuals...**
- ChoicePoint will also have to **submit to comprehensive security audits every two years through 2026.** “

UPDATE: 12/6/06: FTC announced that victims of identity theft as a result of the data breach who had out-of-pocket expenses can now be reimbursed. The claims deadline was Feb. 4, 2007.

FTC – BJ's Wholesale Club

“According to the FTC, BJ's failed to encrypt customer data when transmitted or stored on BJ's computers, kept that data in files accessible using default passwords, and ran insecure, insufficiently monitored wireless networks.

...affected financial institutions filed suit against BJ's to recover damages. According to a May securities and Exchange Commission filing, BJ's recorded charges of **\$7 million in 2004 and an additional \$3 million in 2005 to cover legal costs.**

Under terms of the settlement, BJ's will implement a comprehensive information-security program subject to **third-party audits every other year for the next two decades.**

“

- InformationWeek 6/16/2005

Priceline, Travelocity, and Cingular fined for using adware

Priceline, Travelocity, and Cingular, three high-profile companies that advertised through nuisance adware programs have agreed to pay fines and reform their practices, according to the New York Attorney General.

“Advertisers will now be held responsible when their ads end up on consumers’ computers without full notice and consent,” Andrew Cuomo said. “Advertisers can no longer insulate themselves from liability by turning a blind eye to how their advertisements are delivered, or by placing ads through intermediaries, such as media buyers. New Yorkers have suffered enough with unwanted adware programs and this agreement goes a long way toward clamping down on this odious practice.”

- PressEsc.com January 29, 2007

Spyware - Bank Of America / Joe Lopez lawsuit

“ A Miami businessman is suing Bank of America to recover **\$90,000** that he **claims was stolen and diverted to a bank in Latvia after his computer was infected by a "Trojan horse"** computer virus.

Although consumers are routinely hit with "phishing" E-mails carrying bank logos intended to dupe them into revealing IDs and passwords, this is the first known case of a business customer of a U.S. bank claiming to have suffered a loss as a result of a hacking incident.

In a complaint filed earlier this month, Joe Lopez, owner of a computer and copier supply business, **accused Bank of America of negligence and breach of contract** in not alerting him to the existence of a virus called "coreflood" prior to April 6, 2004, the date the alleged theft took place.” - <http://www.informationweek.com/showArticle.jhtml?articleID=60300288>

Spyware - Sony's DRM Rootkit

Oct 31, 2005 - Mark Russinovich, a security researcher, discovers that Sony's CDs install a rootkit

Nov 3 – Sony releases rootkit remover. Ed Felten dismisses the rootkit remove as junk

Sony's rootkit used to defeat World of Warcraft's security

Nov 15 – Sony's rootkit uninstaller “create huge security hole”

Nov 15 – Dan Kaminsky estimates Sony's rootkit has **infected 568,200 sites, including government and military networks.**

Nov 16 – US-CERT, Dept of Homeland Security, advises: **“Do not install software from sources that you do not expect to contain software, such as an audio CD.”**

Nov 17 – Amazon offers refunds on infected Sony CDs. Nov 21, Army/Airforce exchange as well.

New York, Texas and Florida Attorney Generals sue Sony.

- boingboing.net

Nov 10 – **2 Trojans target Sony's rootkit** -

<http://news.zdnet.co.uk/internet/security/0,39020375,39236720,00.htm>

Attorney fees & expenses exceed \$ 4,000,000. Total costs to Sony unknown. - sonysuit.com

Spyware - Sony's DRM Rootkit Anastacia CD costs retailer 1,500 Euros

Sep 14, 2009 – German Judge orders retailer to pay Plaintiff 1,500 Euros.

- 200 Euros – 20 hours wasted dealing with virus alerts
- 100 Euros – 10 hours for restoring data
- 800 Euros – fees paid by Plaintiff to Computer Expert to repair his network
- 185 Euros – legal costs incurred by plaintiff

“The judge’s assessment was that the CD sold to the plaintiff was faulty, since he should be able to expect that the CD could play on his system without interfering with it.

The court ordered the retailer of the CD to pay damages of 1,200 euros.”

<http://torrentfreak.com/retailer-must-compensate-sony-anti-piracy-rootkit-victim-090914/>

<http://www.heise.de/newsticker/Verkaeufel-muss-Schadensersatz-fuer-Sony-Rootkit-CD-zahlen--/meldung/145233>

ID Theft – Bank Of America & Margaret Harrison

Margaret Harrison, a young wife and mother living in San Diego, first noticed the problem four years ago when she applied for unemployment.

[...] She investigated and found out a laborer named Pablo has been using her Social Security number. **And while Margaret pays for credit monitoring, she says the Equifax credit reporting bureau never noticed the problem until she told the agency.** Now Equifax has put a fraud alert on her account. And then there's this: Last month, the **Bank of America sent her a new debit card bearing her name and Pablo's picture!**

Margaret says the Bank of America claims it can't take any action against Pablo because he pays his bills on time — that her case is in what they call "a reactive state."

- MSNBC Feb 6, 2006 “Hey, that’s not me! A new wrinkle in ID theft”

Fake Receipts, Chinese Style

“ More than 1 million bogus receipts worth 1.05 trillion yuan (147.3 billion U.S. dollars) were confiscated in the case. The national treasury would lose more than 75 billion yuan in tax revenue if the receipts were put into circulation, officials said.”

- <http://english.people.com.cn/90001/90776/6359250.html>

Good News:

Ringleader gets 16 years in jail.

Bad News:

- One of their customers claimed his company was NASDAQ listed and raised \$50M from unsuspecting investors.
- How many of YOUR vendors are claiming financial health using fake receipts?
- How many of YOUR employees padded their expense accounts using fake receipts?

Fake “Cisco” gear

Chinese vendors are selling counterfeit cisco gear at aggressive prices

Per FBI Presentation

- eGlobe Solutions - \$ 788,000 in counterfeit gear
- Todd Richard - \$ 1,000,000 in counterfeit gear

Fake equipment found in:

- US Naval Academy, US Naval Air Warfare Center, US Naval Undersea Warfare Center
- Marine Corps, Air Force, US Air Base (Spangdahelm, Germany)
- Bonneville Power Administration
- General Services Administration (GSA), FAA, FBI, other agencies and universities
- Raytheon
- Lockheed Martin (who violated rules by NOT using a GSA IT Vendor)
- MortgageIT – bought from a Authorized Cisco reseller. 30 WICs faulty.

“Cisco's Brand Protection does NOT coordinate with Cisco's Government Sales”

ATM machines with default passwords

...News reports circulated about a cyber thief who strolled into a gas station in Virginia Beach, Virginia, and, with no special equipment, reprogrammed the mini ATM in the corner to think it had \$5.00 bills in its dispensing tray, instead of \$20.00 bills.

...

Dave Goldsmith, a computer security researcher at Matasano Security began poking around. Based on CNN's video, he identified the ATM as a Tranax Mini Bank 1500 series. [he also found manuals for Triton and another vendor – approx 250,000 ATMs]

...

He then set out to see if he could get a copy of the manual for the apparently-vulnerable machine to find out how the hack worked. Fifteen minutes later, he reported success....[he found]

- * Instructions on how to enter the diagnostic mode.
- * Default passwords
- * Default Combinations For the Safe

- Wired.com, September 20, 2006

TJX (TJ Maxx, Winners, HomeSense) Breach

Information stolen from the systems of massive retailer TJX was being used fraudulently in November 2006 in an \$8 million gift card scheme, one month before TJX officials said they learned of the breach, according to Florida law enforcement officials.

...

Florida officials said the group used the increasingly common tactic of using the bogus credit cards to purchase gift cards and then cashing them at Wal-Mart and Sam's Club stores. The group usually purchased \$400 gift cards because when the gift cards were valued at \$500 or more, they were required to go to customer service and show identification, Pape said.

- eWeek.com March 21, 2007

Arkansas Carpenters Pension Fund, which owns 4,500 shares of TJX stock, said the company rebuffed its request to see documents detailing the safeguards on the company's computer systems and how the company responded to the theft of customer data.

The suit was filed Monday afternoon in Delaware's Court of Chancery, under a law that allows shareholders to sue to get access to corporate documents for certain purposes.

Court papers state the Arkansas pension fund wants the records to see whether TJX's board has been doing its job properly in overseeing the company's handling of customer data.

- Forbes.com, March 20, 2007

Barings, Societe Generale

1995 Barings Bank: \$ 1.4B losses

2008 Societe Generale: \$ 7.1B

“Nick Leeson, [...] said Thursday that a massive fraud by a Société Générale employee showed that **banks still do not have risk-management controls in place.**”

“The first thing that shocked me was not necessarily that it had happened again. **I think rogue trading is probably a daily occurrence among the financial markets,**” Leeson told the British Broadcasting Corp.

[...] **“What they're looking for is profit, profit now, and that tends to be where the money is directed,”** said Leeson”

- International Herald Tribune, <http://www.ihf.com/articles/2008/01/24/business/leeson.php>

“An internal investigation into billions of euros of losses at Societe Generale has found that controls at the French bank “lacked depth”.

The results of the investigation also show that rogue trades were first made back in 2005.

- <http://news.bbc.co.uk/2/hi/business/7255685.stm>

Hannaford Ruling

March 2008:

- Attackers installed custom malware (spyware) to capture data in motion across Hannaford's network
- Hundreds of servers and POS terminals compromised
- 4.2 million records breached – Credit AND Debit cards
- Customers filed class-action lawsuits

May 13, 2009 ruling:

“U.S. District Court Judge Brock Hornby threw out the civil claims against the grocer for its alleged failure to protect card holder data and to notify customers of the breach in a timely fashion. In dismissing the claims, Hornby ruled that without any actual and substantial loss of money or property, consumers could not seek damages.

The only complaint he allowed to stand was from a woman who said she had not been reimbursed by her bank for fraudulent charges on her bank account following the Hannaford breach.

In a 39-page opinion, Hornby wrote that consumers with no fraudulent charges posted to their accounts could not seek damages under Maine law; neither could those who might have had fraudulent charges on their accounts that were later reversed.”

-

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9133075&taxonomyId=17&intsrc=kc_top

They broke the law, your loss!

2008: Malware and/or break-ins compromise 100 million+ records at Heartland Payment Systems.

Jan 2009: Inauguration day – Heartland discloses breach

May 2009: Heartland has spent \$ 12.6 million (and counting) in dealing with the breach.

Feb 2009: Angie's list notices 200% increase in auto-billing transactions being declined. Autp-billing declines increased from 2% to 4%.

May cost them \$ 1 million in lost revenues so far.

“The trouble is that convincing customers who had once set up auto-billing to reestablish that relationship after such a disruption is tricky, as many people simply don't respond well to companies phoning or e-mailing them asking for credit card information”

- http://voices.washingtonpost.com/securityfix/2009/05/heartland_breach_dings_members.html?wprss=securityfix

OpenSocial hacked within 45 minutes

Nov 2, 2007 – hacker compromises Plaxo's Rockyou Opensocial application.

Adds 4 emoticons to reporter's account.

Adds emoticon to Plaxo's VP of Marketing John McCrea's profile.

Same hacker accessed any users's Facebook SuperPoke feed.

- <http://www.techcrunch.com/2007/11/02/first-opensocial-application-hacked-within-45-minutes/>

Facebook of the nation...

Facebook allows developers access to user's full profile.

Every time you choose to add an application, Facebook asks you to confirm that you want to let this program both know who you are and access your information. It's impossible for anyone to add any application without agreeing to this set of terms. Once you click okay, that application can technically access quite a bit of public and private profile information.

While all of the most private information (like your passwords and e-mail addresses) are kept on Facebook servers and require security authentication, a lot of info is available to applications you add.

According to Facebook's Developers Terms of Use, this can include

"... your name, your profile picture, your birthday, your hometown location, your current location, your political views, your activities, your interests, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, copies of photos in your Facebook Site photo albums, and a list of user IDs mapped to your Facebook friends."

- <http://www.removeadware.com.au/articles/facebook-privacy-hackers/>

Facebook your country's security away...

Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net

“ MI6 faced calls for an inquiry last night after an extraordinary lapse of judgment led to the new head of MI6's personal details being plastered over Facebook.

Millions of people could have gained access to compromising photographs of Sir John Sawers and his family on the social networking website. ...“

<http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html>



We Make it Easy (to commit crimes)

Criminals have existed as long as society has. And they always will.

However, we as IT/Security/Business/Government professionals make it easy for them to commit crimes:

- **“It's not MY problem syndrome”**

- Bank Of America ID Theft, UK Banking rules, No liability for software vendors
- Burden for compromise is on the victims (ID theft, house theft, spyware)

- **The selfish gene**

- Sony DRM rootkit, RIAA lawsuits, expired DRM

- **Stupid IT tricks**

- Shipping with default passwords
- Textbooks, documentation showing insecure or poor coding practices

- **Poor Privacy/Security planning**

- ID theft is a growing problem today, because no one thought about limiting scope of SSN usage in 1934
- What do Facebook, MySpace, Gmail teach our kids about privacy?
- Are you looking at security and privacy in a holistic, global manner?

Lose Data, Lose Customers The Ponemon Institute surveyed 14 different companies. The average data loss was 100,000 records. The most costly aspect by far was the loss of existing customers. Here is the breakdown:

| ACTIVITY | DIRECT COSTS | INDIRECT COSTS | LOST CUSTOMER COSTS | TOTAL COSTS |
|-----------------------------------|--------------------|--------------------|---------------------|---------------------|
| Detection & Escalation | | | | |
| - Internal investigation | \$19,000 | \$488,000 | N/A | \$507,000 |
| - Legal consulting | 463,000 | 51,000 | N/A | 514,000 |
| Notification | | | | |
| - Letters | 547,000 | 193,000 | N/A | 740,000 |
| - E-mails | 5,000 | N/A | N/A | 5,000 |
| - Telephone | 913,000 | 105,000 | N/A | 1,018,000 |
| - Published media | 48,000 | N/A | N/A | 48,000 |
| - Web site | 3,000 | N/A | N/A | 3,000 |
| Ex-Post Response | | | | |
| - Mail | 4,000 | 3,000 | N/A | 7,000 |
| - E-mails | 1,000 | 1,000 | N/A | 2,000 |
| - Internal call center | 287,000 | 479,000 | N/A | 766,000 |
| - Outsourced call center | 27,000 | N/A | N/A | 27,000 |
| - Public or investor relations | 289,000 | 14,000 | N/A | 303,000 |
| - Legal defense services | 1,288,000 | N/A | N/A | 1,288,000 |
| - Free or discounted services | 810,000 | N/A | N/A | 810,000 |
| - Criminal investigations | 286,000 | 13,000 | N/A | 299,000 |
| Lost Business | | | | |
| - Lost existing customers | N/A | N/A | 6,728,000 | 6,728,000 |
| - Lost new customers | N/A | N/A | 730,000 | 730,000 |
| AVERAGE COST PER COMPANY | \$4,990,000 | \$1,347,000 | \$7,458,000 | \$13,795,000 |
| PER LOST RECORD COST | \$50 | \$14 | \$75 | \$138 |

SOURCE: PGP CORP.

The Cost of Carelessness 12/5/2005 - <http://www.ciainsight.com/article2/0,1540,1906158,00.asp>

Cost of Breaches 2005-2008

| Year | Direct Cost | Indirect Cost | Lost Customer Cost | Total Costs |
|------|-------------|---------------|--------------------|-------------|
| 2005 | 50 | 14 | 74 | 138 |
| 2006 | 50 | 14 | 118 | 182 |
| 2007 | 50 | 14 | 133 | 197 |
| 2008 | 50 | 14 | 138 | 202 |

* 2009 TOTAL COSTS = \$ 204

Other findings:

Not 1st time for majority of companies – 84% repeat offenders

1st timers cost: \$ 243/record, Experienced Victims: \$ 192/record

Churn Rates: Average 3.6% / Healthcare 6.5% / Financial Services 5.5%

Healthcare cost: \$ 282/record / Retail: \$ 131/record

88% breaches due to insider negligence, 44% due to external parties

Source: <http://www.networkworld.com/news/2009/020209-data-breach.html>

Getting it Right

Medical marijuana advocates estimate that the aggregate annual sales tax revenue that's paid by the approximately 400 dispensaries in California is \$100 million.

- <http://www.npr.org/templates/story/story.php?storyId=89349791>

Cost of War on Drugs in 2010 (so far):
\$ 23 Billion (and counting)

- <http://www.drugsense.org/wodclock.htm>

Getting it Right

“Anesthesiologists pay less for malpractice insurance today, in constant dollars, than they did 20 years ago.

That's mainly because some anesthesiologists chose a path many doctors in other specialties did not. Rather than pushing for laws that would protect them against patient lawsuits, these anesthesiologists focused on improving patient safety.

Their theory: Less harm to patients would mean fewer lawsuits. “

- Deaths dropped from 1 / 5,000 to 1 / 200,000 – 300,000
- Malpractice claims dropped 46% (from \$ 332,280 in 1970 to \$ 179,010 in 1990's!

Premiums dropped 37% from \$ 36,620 to \$ 20,572.

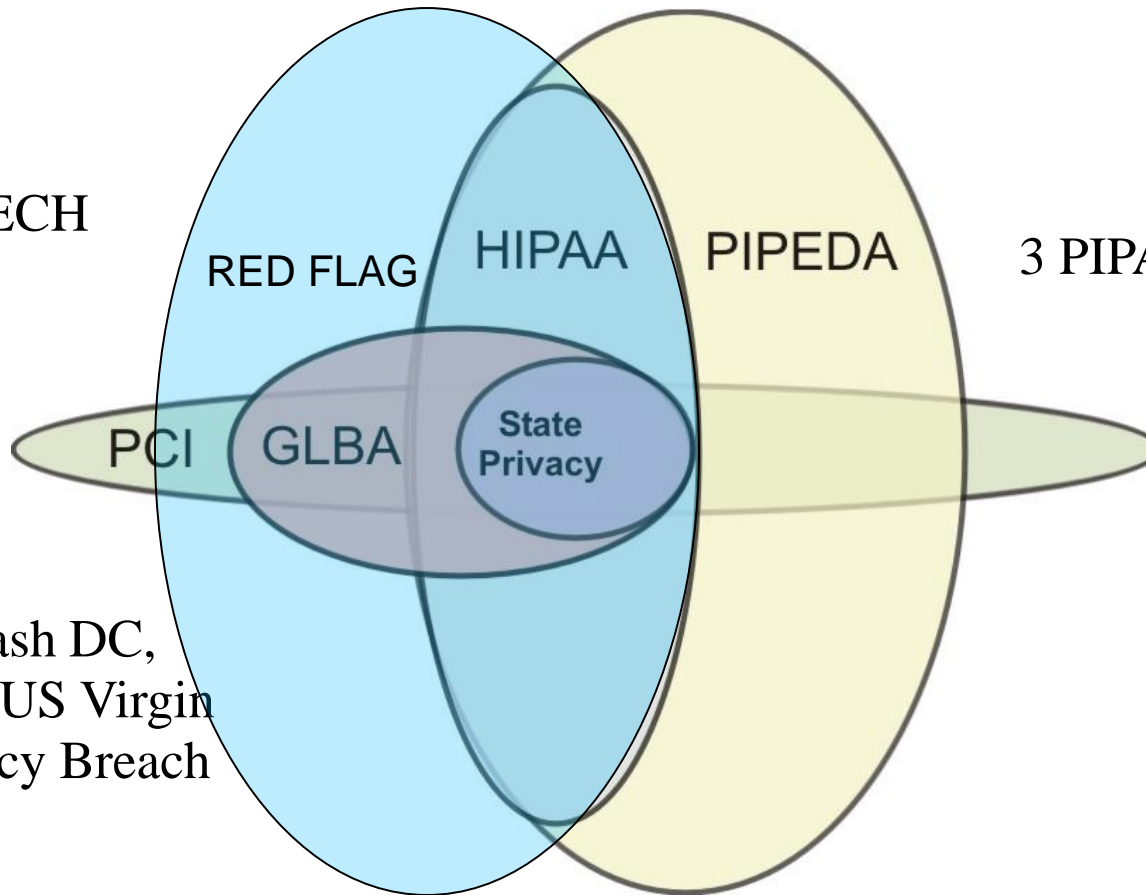
<http://online.wsj.com/article/0,,SB111931728319164845,00.html?mod=home%5Fpage%5Fone%5Fus>

Summary

- Laws aren't static.
- Court cases determine how laws are implemented.
- Revisions to the laws and newer laws expand the compliance landscape.
- FTC and Attorney Generals are expanding the compliance landscape.
- Encrypt, encrypt, encrypt
- Plan to HAVE a breach; and train your staff for it.

This is Job Security!

US
HIPAA/HITECH
GLBA
RED FLAG



Canada
PIPEDA
3 PIPA/PPIPS laws

47 States, Wash DC,
Puerto Rico, US Virgin
Islands Privacy Breach
Laws

Contact Information

Raj Goel, CISSP

Chief Technology Officer

Brainlink International, Inc.

C: 917-685-7731

raj@brainlink.com


www.brainlink.com

www.linkedin.com/in/rajgoel



Questions?

Click on the questions tab on your screen, type in your question, name and e-mail address; then hit submit.



The screenshot shows a web interface with a navigation bar at the top containing four tabs: "Slides", "Questions", "Download", and "Support". The "Questions" tab is selected. Below the navigation bar, the word "Questions" is displayed. A prompt reads "Please submit your question below." followed by a large text area with the placeholder text "Type your question here." and a vertical scrollbar on the right. Below the text area, another prompt reads "Please type your Name" followed by a text input field with the placeholder text "Type your name here". At the bottom of the form is a "Submit" button with a right-pointing arrow icon.