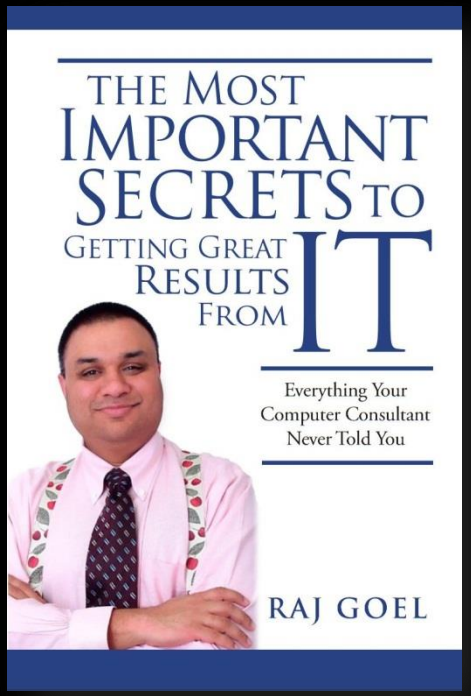
Lessons Learned From The FTC
(Federal Trade Commission, USA)



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

Agenda

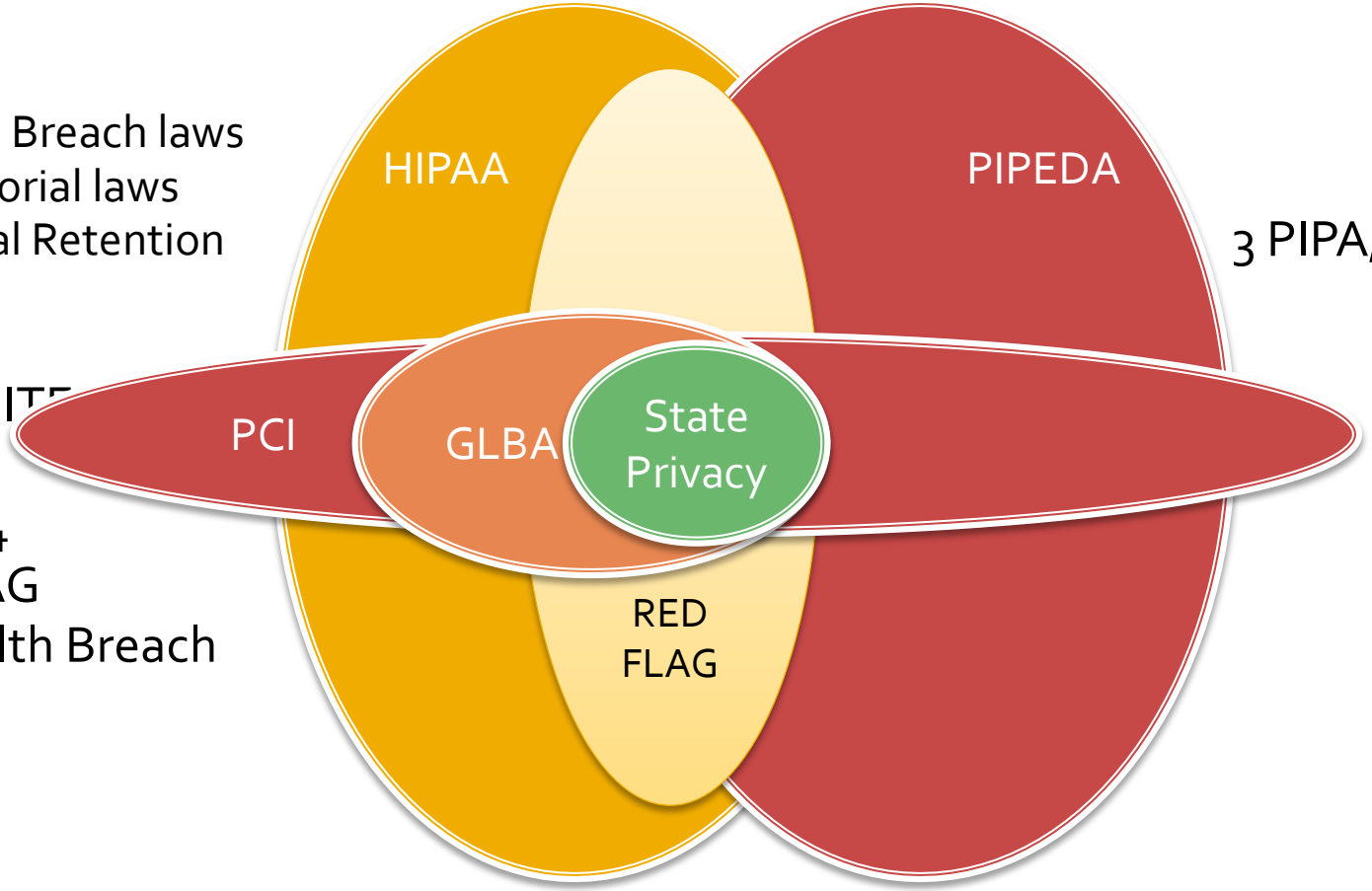
- The cost of Insecurity.
- FTC Case Studies
- Next Steps

Standards Explosion

<u>US</u>

46* State Breach laws
3** Territorial laws
50 Medical Retention
PCI

HIPAA/HITE
GLBA
SOX-404
RED FLAG
FTC Health Breach



<u>Canada</u>

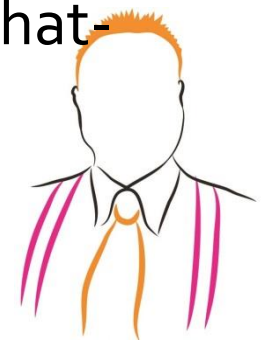
PIPEDA
3 PIPA/PPIPS laws

- *Texas State law covers the 4 states Alabama, Kentucky, New Mexico, and South Dakota
- ** Territories: Washington DC, Puerto Rico, US Virgin Islands

Cost Of Compliance

- According to Gartner:
- 2007
- – Level 1 Merchants spent $ 125,000 in assessments and $ 568,000 for remediation
- – Level 2 - $ 105,000 in assessments and $ 267,000 for remediation
- – Level 3 - $ 44,000 in assessments and $ 81,000 for remediation
- Level 4 – varies

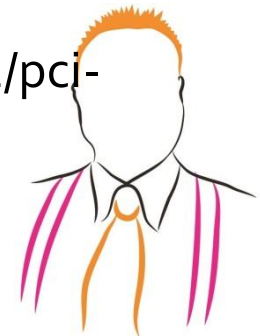
- External IP scan costs ranged from $ 150-$2500/year
- - http://www.braintreepaymentsolutions.com/blog/what-does-it-cost-to-become-pci-compliant



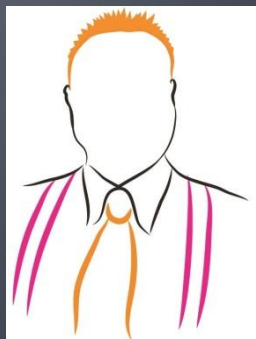
Cost Of Compliance

- According to Ponemon Institute Oct 15, 2010:
- – Level 1 Merchants spent $ 225,000 in assessments , with some spending over $ 500,000 in assessments alone

- 2% of businesses fail the audits
- 41% rely on compensating controls
- IT depts are in charge or security, but business managers control the budget
- VISA, MC & Amex now allow internal audit teams to perform these assessments, not just the QSAs.
- - http://blog.elementps.com/element_payment_solutions/2009/02/pci-compliance-costs.html



Costs of Non-Compliance

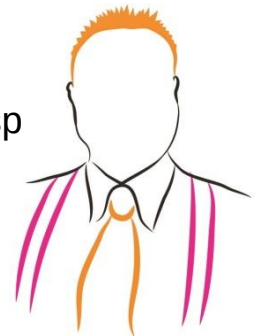


Lose Data, Lose Customers The Ponemon Institute surveyed 14 different companies. The average data loss was 100,000 records. The most costly aspect by far was the loss of existing customers. Here is the breakdown:

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.

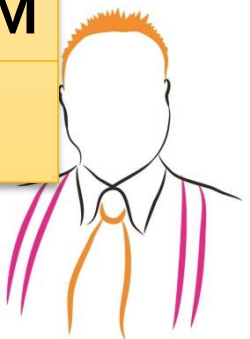
The Cost of Carelessness 12/5/2005 - http://www.cioinsight.com/article2/0,1540,1906158,00.asp



Cost of Breaches – 2005 - 2012

Year	Direct Costs	Indirect Costs	Costs Per Record		Total Cost Of Cleanup
2005	50	88	138		$4.54M
2006	54	128	182		$4.79M
2007	52	145	197		$6.36M
2008	50	152	202		$6.66M
2009	60	144	204		$6.75M
2010	73	141	214		$7.24M
2011	59	135	194		$5.50M

Ponemon Institute 2011 Cost of Data Breach Study



Here's why the problem is even worse

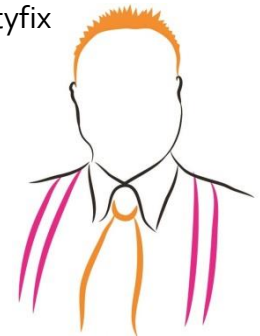
- Corporate Recidivism - 84% repeat offenders
- Virgins pay more: $ 243/record
- Experienced victims pay less: $ 192/record
- Churn Rates: Average 3.6%
  - **Healthcare 4.2% @ $282/Record**
  - **Financial Services 5.6%**
- 88% breaches due to insider negligence
- 44% due to external parties

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. Auto-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

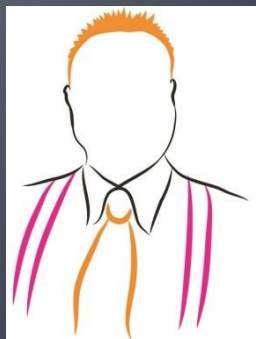


TJX (TJ Maxx, Winners, HomeSense) Breach

- 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

FTC Case Studies



FTC – ToySmart (2000)

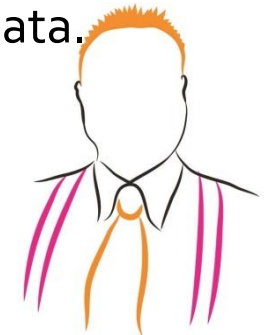
- ToySmart sold educational, non-violent toys and collected information on children while it was in business. It's privacy policies said that it would never share information with 3rd parties.
- Toysmart.com went bankrupt tried to auction off the customer database seperately as an asset of the company.
- "Customer data collected under a privacy agreement should not be auctioned off to the highest bidder," according to Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection. "This settlement protects consumers from a winner-take-all bid in bankruptcy court, ensuring only a family-oriented Web site willing to buy the entire Toysmart Web site has the ability to do so."
- Settlement: Anyone who bought ToySmart must adhere to Toysmart's privacy policies.
- - www.steptoe.com/assets/attachments/937.com

FTC – Microsoft Passport (2002)

- "We believe that Microsoft made a number of misrepresentations, dealing with, one, the overall security of the Passport system and personal information stored on it; two, the security of online purchases made with Passport Wallet; three, the kinds of personal information Microsoft collects of users of the Passport service; and four, how much control parents have over the information collected by Web sites participating in the Kids Passport program," [FTC Chairman] Muris said during the conference call.
- The FTC outlined its findings in a six-page complaint. Many of the problems resulted from Microsoft failing to adhere to its own privacy statements about Passport, Passport Wallet or Kids Passport.

- No penalties, 20 years of reporting to FTC required.
- For 5 years, MS to submit advertising materials and all other documentation pertaining to collection or retention of consumer data.

http://news.cnet.com/2100-1001-948922.html



FTC - DSW (2005)

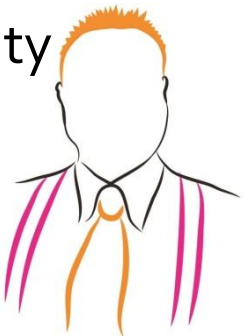
- "Shoe retailer DSW Inc. agreed to beef up its computer security to settle U.S. charges that it didn't adequately protect customers' credit cards and checking accounts,...
- The FTC said the company engaged in an unfair business practice because it created unnecessary risks by storing customer information 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 – BJ's Wholesale Club (2005)

- "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

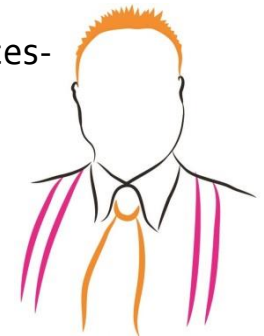
FTC - Choicepoint (2006)

- "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. "
- - ComputerWorld.com 01/26/2006



FTC - Sears/Kmart (2009)

- In 2009, Sears.com and Kmart.com websites offered to 15% of their visitors, via a pop-up, a chance to "talk directly to the retailer". This pop-up installed spyware on their customer's (or potential customer's) computers!
- Consumers probably didn't realize that by "new" and "different," the advertisement meant "all-seeing" and "invasive." Indeed, this software monitored both online and offline behavior, peering into online secure sessions and culling information from consumers' email subject and recipients, online bank statements, drug prescription records, video rental records, and similar histories and accounts. Customers effectively (and blindly) sold their privacy by agreeing to a lengthy terms of service agreement that showed up at the end of a long registration process. The agreement was presented in a small "scroll box"; consumers could only see ten lines of the policy at a time and not until the 75th line could the user find any description of the invasive tracking.
- Sears was required to delete all data collected under this program.
  - - http://www.cdt.org/blogs/erica-newland/ftc-finalizes-terms-sears-deceptive-practices-settlement



FTC & OCR – CVS HIPAA (2009)

- Largest, joint coordination between OCR, HHS and FTC.

- Reviews by OCR and the FTC indicated that:
- CVS failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process; and
- CVS failed to adequately train employees on how to dispose of such information properly.

- Under the HHS resolution agreement, CVS agreed to pay a $2.25 million resolution amount and implement a robust corrective action plan that requires Privacy Rule compliant policies and procedures for safeguarding patient information during disposal, employee training and employee sanctions for noncompliance.
- HHS and FTC also will require CVS to actively monitor its compliance with the resolution agreement and FTC consent order. The monitoring requirement specifies that CVS must engage a qualified independent third party to conduct assessments of CVS compliance and render reports to the federal agencies. The HHS corrective action plan will be in place for three years; the FTC requires monitoring for 20 years.
- http://www.hhs.gov/news/press/2009pres/02/20090218a.html

FTC – EchoMetrix/Pulse(2010)

- Parents paid Echometrix $ 3.99/mo for Sentry Parental Controls. This allowed parents to monitor web surfing, IM, email, etc.
- June 2009 – Echometrix launches Pulse – a "market research" program that analyzed web traffic, social media, IM, etc so that marketers could find out what consumers were saying about their products or services. Companies that bought Pulse could retrieve actuals IM, chat and forum posts.

- FTC charged that EchoMetrix failed to adequately inform parents that information collected by Sentry would be sold to marketers. EchoMetrix had vague statements buried in their EULA (sound familiar??)

- Settlement: - EchoMetrix must destroy the info from Sentry that was copied into the Pulse Database. It cannot use Sentry data for any other purposes.
- http://business.ftc.gov/blog/2010/12/ftc%E2%80%99s-echometrix-settlement-eula-ppreciate-guidance-privacy-disclosures

FTC – US Search (2010)

- US Search charged sutomers $10 to "lock their records" and prevent them from showing up in searches online.
- In it's settlement, US Search had to refund fees to 5000 customers.
- Commissioner Brill said industry should consider providing consumers with meaningful notice about information brokers' practices, a reasonable means to access and correct consumers' information, and a reasonable mechanism to opt out of these databases.
- http://www.ftc.gov/opa/2011/03/ussearch.shtm

FTC – CyberSpy Software (2010)

- CyberSpy sold a keylogger, marketed towards parents, spouses and colleagues. They provided their clients with detailed instructions on how to disguise RemoteSpy as an innocouos program.

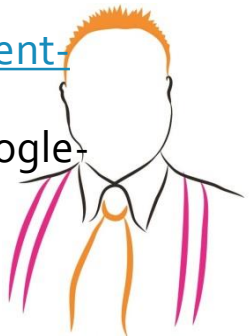
Settlement:

- not assist purchasers in falsely representing that the software is an innocuous file;
- cause an installation notice to be displayed which must include a description of the nature and function of the program and to which the user must expressly consent;
- cause an icon to appear in the task bar on the user's desktop when the software is running, unless the icon is disabled by a person with administrative rights to the computer;
- inform purchasers that improper use of the program may violate state or federal law;
- take measures to reduce the risk that the spyware is misused, including license monitoring and policing affiliates;
- encrypt data collected by the program that is transferred over the internet; and
- remove legacy versions of the software from computers on which it was previously installed

http://privacylaw.proskauer.com/2010/06/articles/spyware/ftc-settlement-bars-marketing-of-spyware-for-illegal-uses/.

FTC – Google Buzz (2011)

- 2009 – Google released Buzz – integrated into Gmail, without warning or user consent.
- 2011 – FTC v Google settlement
- The first time a comprehensive privacy program (as opposed to a comprehensive security program) was required by an FTC consent decree.
- The first time the FTC has enforced the US-EU Safe Harbor Principles for substantive non-compliance.
- No monetary penalties, but Google is required to
- Implement a comprehensive privacy program
- Conduct regular, independent audits for the next 20 years
- FTC also noted that the Google Wi-Fi sniffing would have constituted a violation of this settlement.
  - http://www.huffingtonpost.com/2011/03/30/googles-ftc-privacy-settlement-buzz_n_842490.html
  - http://privacylaw.proskauer.com/2011/04/articles/ftc-enforcement/ftcgoogle-settlement-marks-two-firsts-in-ftc-privacy-enforcement/

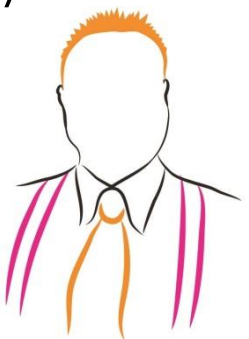


FTC – Chitika (2011)

- Chitika buys ad space, and places cookies on end-users browsers.

- When consumers opt-ed out, Chitika stopped displaying ads for 10 days.
- After 10 days, Chitika re-started displaying ads to opt-out consumers.

- FTC charged Chitika with engaging in "deceptive practices"
- Per the settlement, Chitika must:
- Stop making misleading statements about it's data collection policies
- Every ad must display clear opt-out links with opt-out for 5 years
- Destroy all personally identifiable information collected during defective opt-out
- Chitika must alert consumers that their previous opt-out was not valid.
- - http://www.infolawgroup.com/2011/03/articles/enforcement/privacy-enforcement-update-ftc-settles-with-twitter-and-chitika/



FTC – Twitter (2011)

- Twitter promised that "private tweets" were safe.
- In 2009, Hackers broke into twitter and make tweets public.

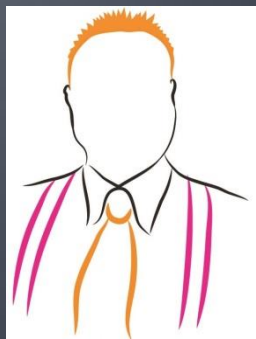
- FTC alleged that serious lapses in Twitter's security allowed hackers to penetrate Twitter. (Hackers brute forced administrative passwords after trying thousands of passwords against Twitter's login page).

- The settlement
- Requires Twitter to update it's privacy & security policies
- Twitter must honor privacy choices made by consumers
- Independent auditor must assess Twitter's security every other year for 10 years
  - http://www.ftc.gov/opa/2011/03/twitter.shtm

FTC & OCR – Riteaid HIPAA (2011)

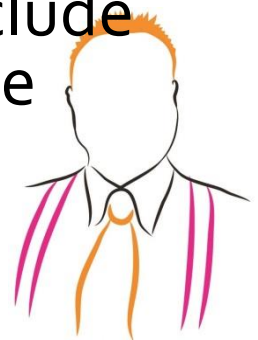
- OCR and the FTC indicated that:
- Rite Aid failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process;
- Rite Aid failed to adequately train employees on how to dispose of such information properly; and
- Rite Aid did not maintain a sanctions policy for members of its workforce who failed to properly dispose of patient information.
- Rite Aid agreed to pay a $1 million resolution amount to HHS and must implement a strong corrective action program that includes:
- Revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;
- Training workforce members on these new requirements;
- Conducting internal monitoring; and
- Engaging a qualified, independent third-party assessor to conduct compliance reviews and render reports to HHS.
    - Rite Aid has also agreed to external independent assessments of its pharmacy stores' compliance with the FTC consent order. The HHS corrective action plan will be in place for three years; the FTC order will be in place for 20 years.

Next Steps



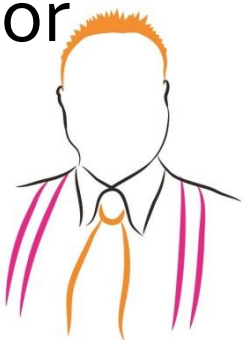
FTC Health Breach Rule

- "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"



Learn from 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

- 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 =
- "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.
- Can you apply this principle to ALL data in your company's possession?

FTC's RED FLAG Rules

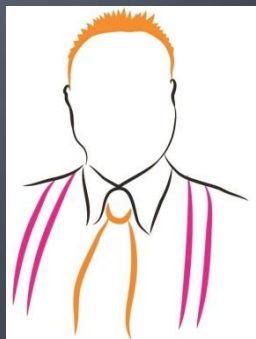
- What are the "red flags"?
- Warning signs that ID theft may, or has, occurred.

- "Financial Institutions" and "Creditors" must develop and implement written ID theft prevention programs that:
- Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;
- Detect Red Flags that have been incorporated into its program;
- Respond appropriately to any Red Flags that are detected;
- 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

Success Stories



John Snow – London Cholera 1849-1854

- 1830 – Cholera kills 60,000 deaths
- 1849 – He identified GEOGRAPHIC CLUSTERS of outbreaks
- Identified that the WATER SOURCE was the vector long before CHOLERA GERM was identified
- Those with BETTER water sources were 20 times LESS LIKELY to die
- He did door-to-door validation/census to check water sources and his data
- RESULT: London took APPROPRIATE public health safety measures to control contaminated public water sources

Dr. Samelweis – 1840s

- During 1840's many women died of childbed fever. Often the child became ill & died as well

- Dr. Samelweis noticed that of the 2 clinics he was managing, one had a HIGHER rate of mortality than the other
- Mothers were ill during birth or up to 36 hours afterwards
- Observed that problem started during the examination of the mother during dilation
- The deaths were caused by MEDICAL STUDENTS who had just come from the morgue after performing autopsies and then proceeded to conduct pelvic examinations on laboring mothers.

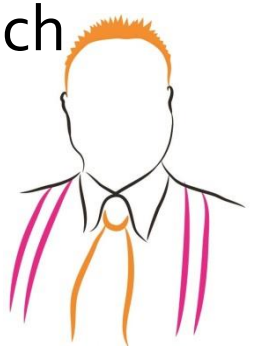
- This **contradicted over 2000 YEARS of medical dogma** and practices since Hippocrates.
- He instituted hand-washing of medical staff between each procedure

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

- What was your overall IT spending last year? How much on questionable security products?



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

Air Force demanded, and purchased, SECURE Desktops

- 2006 – After years of attacks, and dealing with a hodge-podge of desktop and server configurations, The US Air Force develops the Secure Desktop Configuration standard. All vendors are required to sell computers to the USAF (and later DOD, other government agencies) with standardized, locked down configurations of:
  - Windows
  - MS Office
  - Adobe Reader
  - Norton AV
  - Etc
- US Dept Of Energy requires Oracle to deliver it's databases in a secure configuration developed by the Center for Internet Security (www.cisecurity.org)

Compliance Roadmap

Oversight		
Administrative	Training	Technical
Remediation		Staff Augmentation
GAP Analysis	Onsite Training	Remediation
Advisory	Technical Training	Full Audit
Custom Policies	Training Set (1-10)	POP Review (Personnel, Operations, Procedures)
Base Policy Development		

Shameless Self-Promo

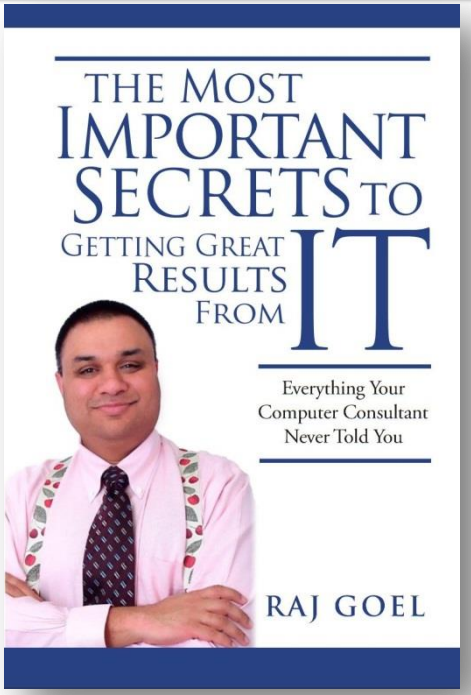
- Raj Goel provides COMMON SENSE BASED IT Security and Privacy Breach law compliance audits
- Information Security Audits
- IT Consulting for Healthcare
- If you like what you're hearing, contact me!
- www.**RajGoel**.com
- www.**ITSecurityConsultant**.com

Contact Information

Raj Goel, CISSP

Chief Technology Officer
Brainlink International, Inc.

917-685-7731
raj@brainlink.com
www.RajGoel.com
www.linkedin.com/in/rajgoel



Author of "**The Most Important Secrets To Getting Great Results From IT**"
http://www.amazon.com/gp/product/0984424814

2nd book **"An Overview Of HIPAA, HITECH, STATE BREACH NOTIFICATION LAWS, PCI-DSS And Attorney Ethics Rule 1.6" coming soon!**