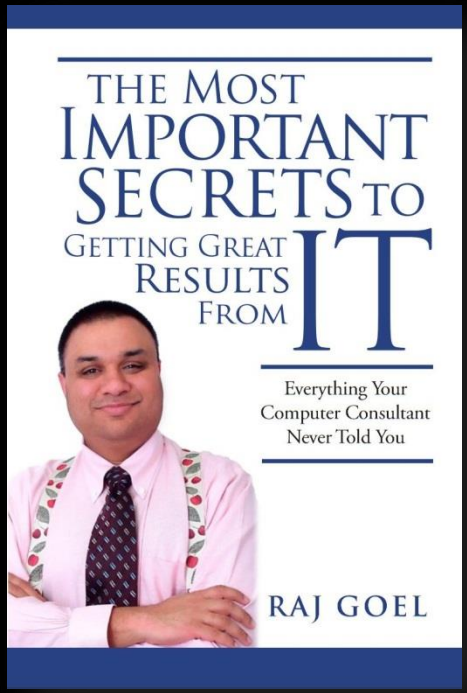
What Every MSP Needs To Know About Compliance

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



datto 2013
WASHINGTON DC

Raj Goel, CISSP

Raj Goel, CISSP, is an Oracle and Solaris expert and he has over 25 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/HITECH, PCI-DSS Credit Card Security, Disaster Recovery, Information Security and other technology and business issues, addressing diverse audiences including technologists, policy-makers, front-line workers and corporate executives.

A internationally known expert, Raj has appeared in over 30 magazine and newspaper articles worldwide, including ***Information Security Magazine***, ***PenTest***, ***CSOOnline***, ***Entrepreneur Magazine***, ***Business2.0*** *and* ***InformationWeek***, and on television including ***CNNfn***, ***Geraldo At Large*** , **PBS** and **WPIX11.**

Raj has presented at:

- **ISC²** conferences
- **ASIS International** conferences
- **BrightTalk** conferences
- Medical Conferences
- Legal Conferences
- **GBATA 2012 & 2013** (keynote speaker)
- **The Hague, Netherlands NCSC.NL 2013** (plenary speaker)
- **GBATA 2013 Helsinki** – Keynote Speaker
- **ICT Curacao** – Keynote Speaker

Media Appearances

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

GBATA | Global Business and Technology Association™

CSO
BUSINESS RISK LEADERSHIP

ASIS INTERNATIONAL
Advancing Security Worldwide®

The New York Times

Entrepreneur

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY℠

BrightTALK™

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

FOX NEWS Channel

CyberHood Watch

PBS

DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES
OFFICE OF COUNTER TERRORISM
NEW YORK STATE

NYIT MAGAZINE

CNNfn
the financial network

PenTest
magazine

ITV

NEW YORK COUNTY
NYCLA
LAWYERS' ASSOCIATION

Disclaimer, Legal Stuff

- This is not legal advice.
- This is not compliance advice.
- This is not an endorsement (or lack there of) of any vendor, product or service

- No product, Service or Vendor can make you compliant. Only you, your people and how you implement can do that.

Raj's Law

- Compliance is
  - 20% Technology
  - 30% Procedures & Processes
  - 50% People

Agenda

- Regulatory Overview
  - HIPAA / HITECH / Omnibus Update
  - FTC Health Breach Rule
  - PCI-DSS
  - 5 Common HIPAA Mistakes
  - Top 7 reasons organizations FAIL Security Assessments
- Case Studies
- Food For Thought
- Guidance
- Success Stories
- Market Opportunity

Every Law has 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

What's HIPAA?

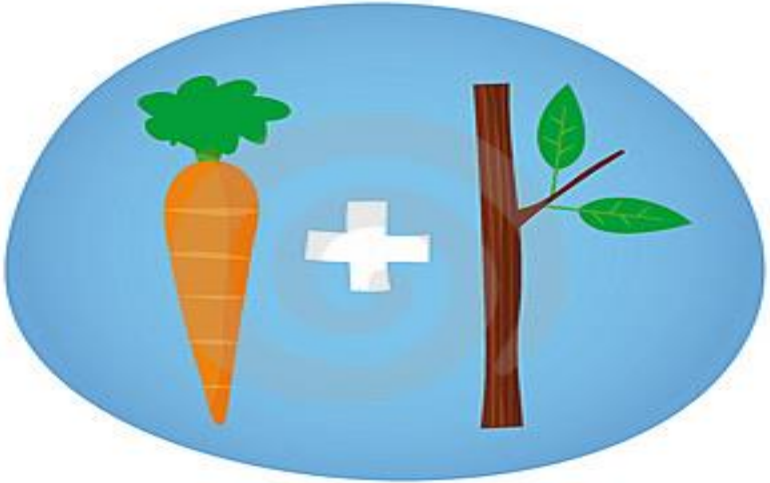
- Health Insurance Portability and Accountability Act of 1996
- 3 Sections
  - Privacy
  - Transactions Code Sets
  - Security
- Goals:
  - Reduce Administrative overhead costs ($0.26)
  - Reduce Fraud & Abuse ($0.11)
  - Protect privacy

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

HITECH Changes to HIPAA

Implement "meaningful use" EHRs and get Federal Grants



Greater Penalties

Larger Scope

Closed Loopholes

HITECH Changes to HIPAA

- Increased Penalties (willful neglect penalties have no limit!)
- Secretary of HHS is required to fully investigate is initial complaint indicates possible willful neglect* (ignorance is no longer a defence)
- State AGs may also sue HIPAA violators
- HIPAA provisions directly apply to Business Associates
- Notify customers, HHS, Media within 60 days
- Lose > 500 records, join HHS' Hall Of Shame!
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

HIPAA Omnibus Update

- The Omnibus Rule expands the definition of "business associate" to include entities that transmit and need routine access to PHI (e.g., Health Information Organizations, E-Prescribing Gateways); vendors of personal health records who serve covered entities; subcontractors who create, receive, maintain or transmit PHI on behalf of business associates; and entities that, on behalf of a covered entity or organized health care arrangement ("OHCA") handle PHI for patient safety activities carried out by or on behalf of a Patient Safety Organization or a health care provider.

HIPAA Omnibus Update

- Do you have BAA's with your

- IT provider?
- Copier Provider?
- Billing Company?
- Attorneys who handle malpractice, third party, workers comp, etc cases?
- VOIP, Voicemail Providers?
- Medical Equipment & Software providers?

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"

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

5 Common HIPAA/HITECH Mistakes

1. Not taking HIPAA/HITECH seriously
2. Sharing Documents with Attorneys over Dropbox
3. Attorneys & IT providers who do NOT take HIPAA seriously.
4. Texting with patients
5. Using Google Docs, Google or Yahoo Calendar for scheduling appointments

Top 7 reasons why practices fail Security Assessments

- They do NOT

1. Regularly test security systems and processes
2. Protect Stored Data
3. Assign a Unique ID to each person with computer access
4. Track and Monitor ALL Access To Network Resources
5. Install and Maintain A Firewall
6. Update Systems
7. Have an **adequate and tested** Disaster Recovery and Business Continuity plan in place

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 Opportunity is even better!

- 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

Case Studies

Phoenix Cardiac Surgery, P.C. - $ 100,000 fine

- (a) From April 14, 2003 to October 21, 2009, Covered Entity did not provide and document training of each workforce member on required policies and procedures with respect to PHI as necessary and appropriate for each workforce member to carry out his/her function within the Covered Entity.
- (b) From September 1, 2005 until November 1, 2009, Covered Entity failed to have in place appropriate and reasonable administrative and technical safeguards to protect the privacy of protected health information (PHI). These failures contributed to and are evidenced by the following acts or omissions:
  - (i) From July 3, 2007 until February 6, 2009, Covered Entity posted over 1,000 separate entries of ePHI on a publicly accessible, Internet-based calendar; and
  - (ii) From September 1, 2005 until November 1, 2009, Covered Entity daily transmitted ePHI from an Internet-based email account to workforce members' personal Internet-based email accounts.

Accretive Health
$2.5 Million Fine, $23-25M lost revenue

- Minnesota Attorney General sanctioned Accretive Health, a [revenue cycle management] service provider that was involved in a security breach affecting patients of two hospitals that engaged Accretive to provide debt collection and other services. The resultant lawsuit by the AG pursued claims related to questionable debt collection practices, but also included multiple alleged HIPAA violations, as detailed in our earlier alert. Without admitting any of the allegations, Accretive Health has just agreed to settle this lawsuit on the following terms:
- · Accretive Health will pay $2.5 million to the State of Minnesota as part of a restitution fund to compensate affected patients.
- · By November 1 of this year, Accretive Health must cease operations in Minnesota for a two-year period, thereby cutting off $23-25 million in projected annual revenues for the company. It must also destroy or return all health and financial information of its Minnesota clients within 60 days of closing its operations in the State and pay a consultant to verify this action has been taken.
- · If Accretive Health wants to do business in Minnesota after its two-year exclusion period, it must first procure the consent of the State's Attorney General, and will be subject to their oversight for four years.
- At least one of the three hospitals in the State that engaged Accretive Health ended its relationship with the company before any settlement was reached, and Accretive Health's vice president and corporate controller resigned. The Attorney General's office has also referred evidence in the form of patient affidavits it collected in its investigation of this matter to the Centers for Medicare and Medicaid Services for potential enforcement actions under the federal Emergency Medical Treatment and Active Labor Act against the hospitals formerly doing business with Accretive Health.

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 was 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

- "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

Drive By looting #1 - TJX (TJ Maxx, Winners, HomeSense) Breach leads to Walmart losses

- 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

Drive-by Looting #2 – Heartland & Angie's List

- 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.

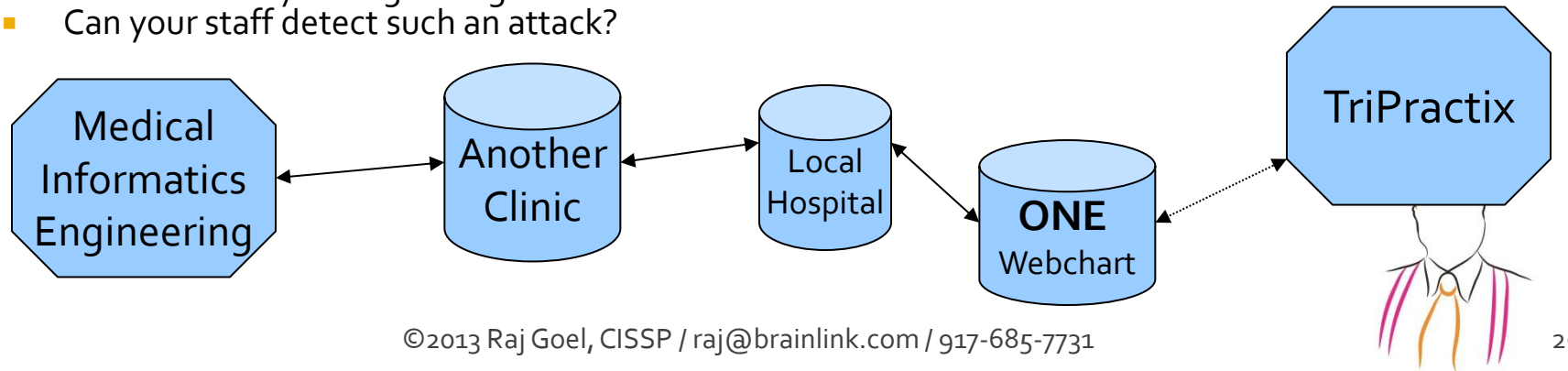
- "The trouble is that convincing customers who had once set up auto-billing to reestablish that relationship after such a disruption is tricky, as many people simply don't respond well to companies phoning or e-mailing them asking for credit card information"

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

Food for Thought

Case Study - Orthopaedics Northeast

- MIE installed & used to support Webchart at ONE
- ONE experienced performance problems in WebChart
- Analysis led to discovery of backdoor – MIE username bypassess all controls, provides direct access to DB
- Hacker used backdoor to create additional, normal accounts
- ONE logs show attacks came from local hospital
- Hospital logs show attack originating from another clinic
- Another's Clinic's logs show attack came from MIE
- MIE claims they did not install the backdoor, or attack ONE.
- Who did? Are your logs this good?
- Can your staff detect such an attack?



Spyware - Israel's TrojanGate

- "Executives of top telecom firms accused of spying on each other. A jealous ex-husband suspected of monitoring his former in-laws. Private investigators implicated in computer-hacking-for-hire; one now involved in a possible attempted suicide. So much bad publicity, government officials worry it might impact the entire nation's economy.

- Published reports indicate mountains of documents have been stolen from dozens of top Israeli firms. Some 100 servers loaded with stolen data have been seized."

- - MSNBC, June 9, 2005 http://www.msnbc.msn.com/id/8145520/

Guidance

IBM bans Dropbox, Siri, iCloud

- IBM has banned employees from using Dropbox and Apple's iCloud at work as it claws back permission to use third-party cloud services. The rethink has also resulted in a edict against the iPhone 4S's Siri voice recognition technology at Big Blue.
- Jeanette Horan, IBM's chief information officer, told MIT's Technology Review that the restrictions had been applied following a review of IBM's Bring Your Own Device BYOD Policy, introduced in 2010. IBM still supplies BlackBerrys to about 40,000 of its 400,000 employees, but a further 80,000 others now access its intranet using rival smartphones and tablets, including kit they purchased themselves. The [BYOD - ed.] initiative has not yielded anticipated cost reductions even though it has created various security headaches.
- An internal survey of IBM workers discovered they were "blissfully unaware" about the security risks from popular apps, according to Horan. In some cases, staff forwarded internal corporate emails to webmail inboxes, potentially pushing sensitive information beyond Big Blue's security perimeter.

- http://www.theregister.co.uk/2012/05/25/ibm_bans_dropbox_siri/

Implement the SANS Top 20

- 1: Inventory of Authorized and Unauthorized Devices
- 2: Inventory of Authorized and Unauthorized Software
- 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Malware Defenses
- 6: Application Software Security
- 7: Wireless Device Control
- 8: Data Recovery Capability
- 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- 11: Limitation and Control of Network Ports, Protocols, and Services
- 12: Controlled Use of Administrative Privileges
- 13: Boundary Defense
- 14: Maintenance, Monitoring, and Analysis of Security Audit Logs
- 15: Controlled Access Based on the Need to Know
- 16: Account Monitoring and Control
- 17: Data Loss Prevention
- 18: Incident Response Capability
- 19: Secure Network Engineering
- 20: Penetration Tests and Red Team Exercises

http://www.sans.org/critical-security-controls/

Implement the AusCERT Top 4

- The top four mitigations are:
-
- patching third party applications;
- patching operating systems;
- minimising administrative privileges;
- application whitelisting.

http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm
http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf

Does this stuff actually work?

Anesthesiologists reduce malpractice premiums 37%

- "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,,SB11193172831916484 5,00.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)

Retailer saves MILLIONS thru PCI Compliance

- One of Brainlink's clients executes several million transactions per month.
- As part of the PCI compliance process, the IT team recommended upgrading the database storage servers and implementing column-level encryption.
- These and other upgrades saved 1/100th of a second PER transaction.
- Client achieved break-even ROI on the entire multi-million dollar PCI compliance and IT upgrades budget within 13 months.

Summary

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

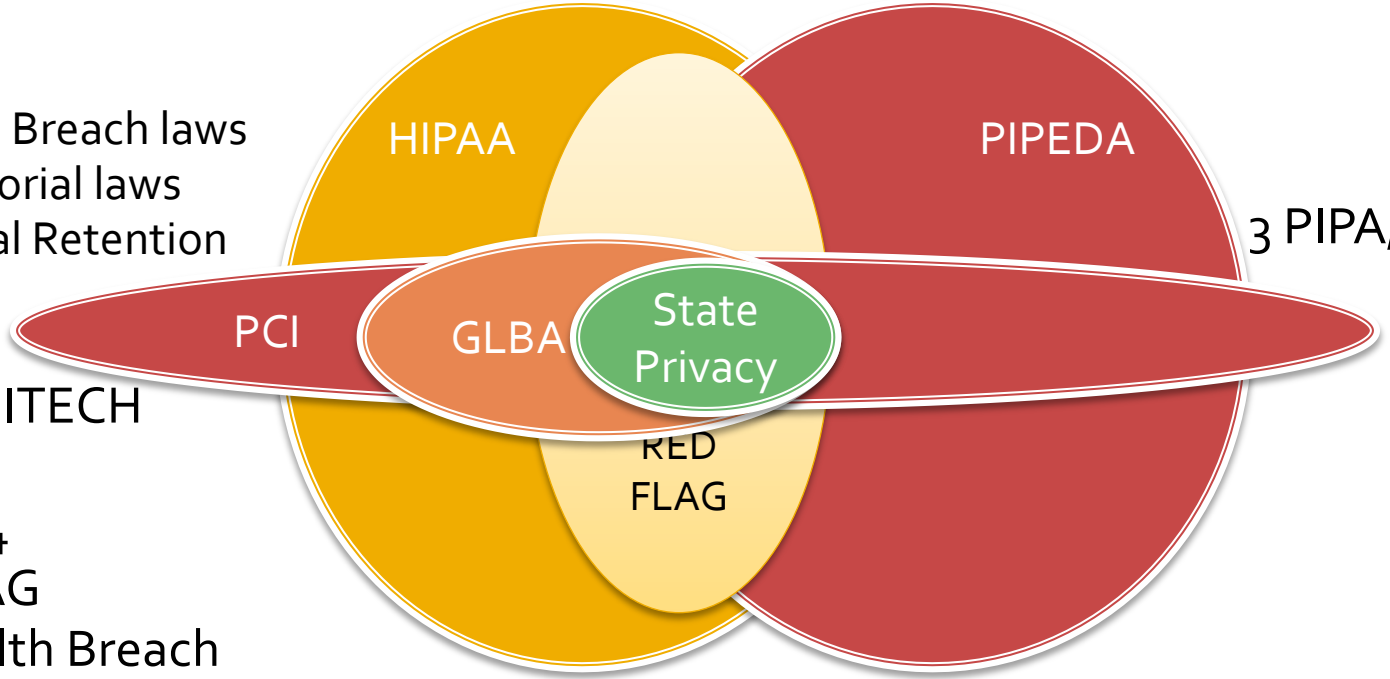
Market Opportunity

105 Laws and Standards

<u>US</u>

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

HIPAA/HITECH
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

Health Care IT != Regular IT

- Based on historical trends, I forecast
  - Consolidation of Healthcare
  - A specialization in the MSP field within next 5 years
  - Rise of HealthMSPs

Current Opportunities

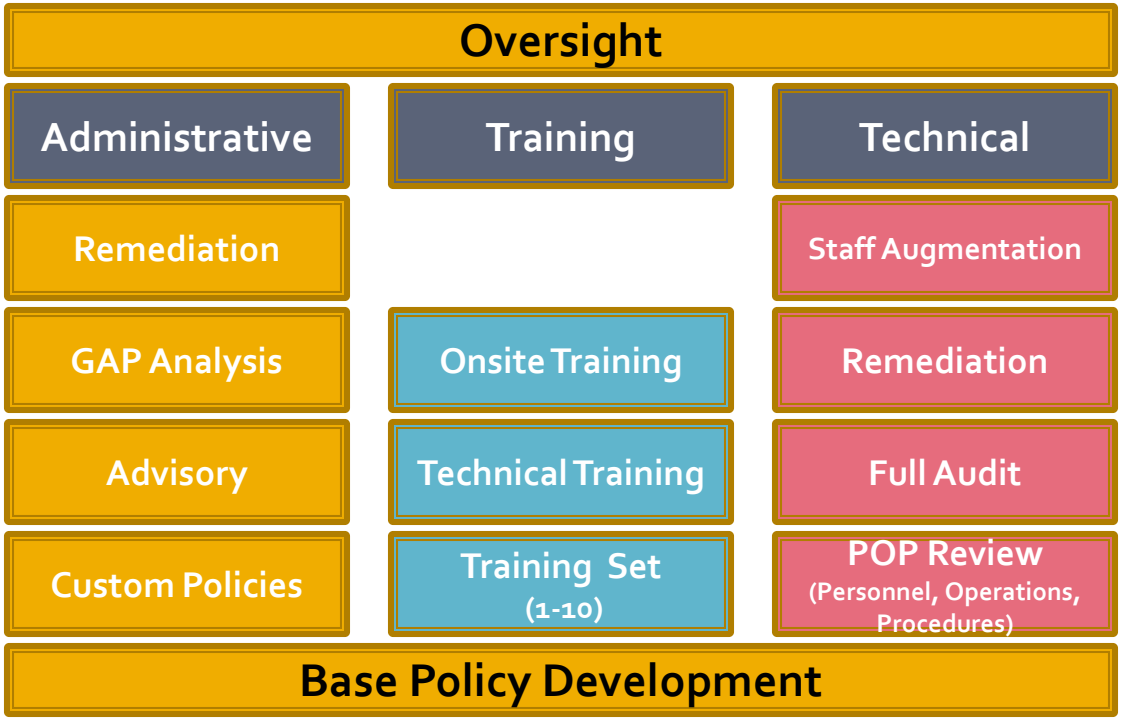
- <$5M – firms do NOT care about compliance.
  - Current MSP tools do NOT have compliance and auditing built-in
  - Several practices, MSPs and Vendors will have to be sued
- $5M-$20M – Audits, Project Work, Expert Assistance
  - Underserved, overlooked
- $20M-$500M – Ripe for Cherry Picking
- You need an experienced partner and CISSP to penetrate these accounts

Additional Resources

http://www.RajGoel.com/Compliance-notes/

- Copy of these slides
- Articles you can use in your newsletters
- HIPAA Wall of Shame
- Past Newsletters
- Attorney Guidance for BA's

Compliance Roadmap



Need Help?

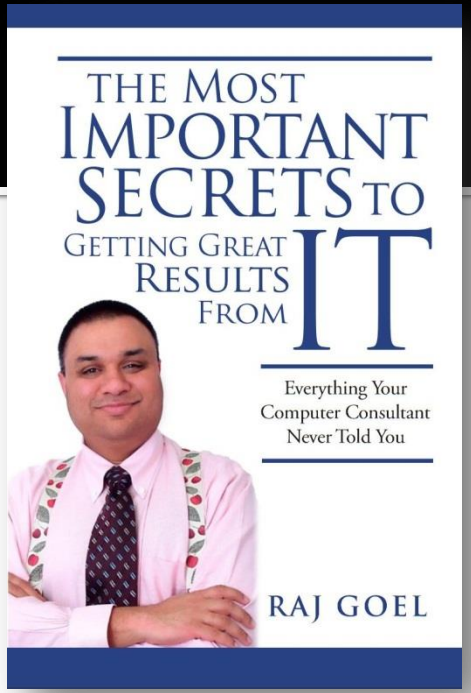
www.ITSecurityConsultant.com

Contact Info

Raj Goel, CISSP

Founder & 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!**