RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO1-T10

Restoring Order: The Inevitable Evolution of IT Security Regulation

Stephen Treglia, JD, HCISPP

Legal Counsel
Absolute Software Corporation
@stevetreglia

Intro into the depth of the problem

- These are the figures being bandied about lately
- Includes everything
- Personpower costs, regulatory penalties, lawsuits costs & damages, damage to brand & reputation, etc.

Goals of today's presentation

- Provide insight as to the current escalation of data privacy laws and regulations
- Provide insight for those who wonder why all the regulatory fuss
- Explain the history and evolution of privacy regulation
- Give you insight as to future course of privacy regulation
- Provide concepts & real processes to best keep your mobile devices safe and compliant with privacy laws and regulations

Who am I to present this?

- **Nov. 2010** Legal Counsel, Absolute Investigations since
- **1980-2010** Prosecutor in New York
- **1985-1995** Investigated/prosecuted Organized Crime
- **1986** Started using computers
- **1996** Started investigating/prosecuting computer crime
- Created one of first Technology Crime Units in **1997**, headed it to **2010**
- **2006** Started investigating/prosecuting Absolute cases
- **Since November 2010** legal advisor to Absolute's staff of investigators and data analysts & HIPAA compliance officer for Investigations
- Collective former law enforcement experience of Investigations Team is **900** years. Recovered **35,000+** stolen mobile devices from **112** different countries.
- Acquired ISC2's HCISPP certification in March, 2015

Typical lawyer disclaimer

Nothing said during this presentation should be considered legal advice. This is intended to be nothing more than a general analysis of broad legal principles in a scholastic setting. Legal advice is properly provided only when it is more finely attuned to specific facts and specific issues in a specific, real-life situation, which will not be provided at this presentation. When seeking legal advice in this area of law, look to counsel who is both knowledgeable in this area of law and fully understands how your business or enterprise operates.

2014 – “Year of the Breach”

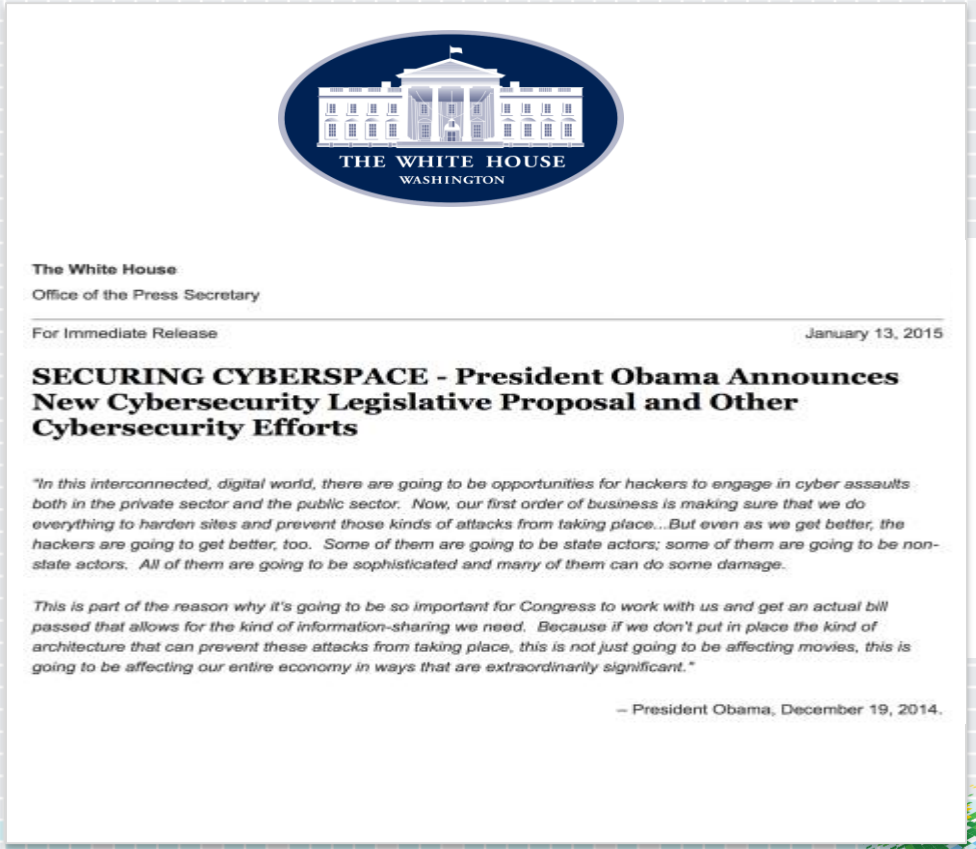
- Started with consequences of the Target hack (currently estimated at over 110 million accounts breached)
- First of several POS attacks
- Neiman-Marcus, Michaels, PF Chang’s
- Couple of Russian teens accused of creating malware called Black POS
- C-suite members lost jobs
- Massive lawsuits pending
- By the time of the Home Depot breach, people were bored with the story

Then along came Sony and the Guardians of Peace

- Series of financial institution attacks from summer-fall 2014
- The year ends with a major media cyberattack – Sony's media group
- Dispute over whether North Korean-sponsored or insider attack
- Purportedly malware attack – Destover
- Once through the firewall, accessed numerous areas of the network
- Contracts, scripts, employee health information, internal emails

Spurring government to respond

- White House press release – 1/13/15 (reiterated at 1/20 State of Union address)
- Cybersecurity solutions a centerpiece of his agenda going forward
- Claims enhanced legislation, funding, enforcement all coming
- A proposal with support of “both sides of the aisle”
- New agencies and proposals already begun in 2015



THE WHITE HOUSE
WASHINGTON

The White House
Office of the Press Secretary

For Immediate Release — January 13, 2015

SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts

"In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place...But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.

This is part of the reason why it's going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant."

– President Obama, December 19, 2014.

Even in my home state

- NY – the financial capital of the world
- AG notes there is currently no law in NY requiring businesses to institute cyber security
- Also proposes expanding the categories of data that must be protected to include email passwords, among others
- Also proposes HIPAA-type data protection
- Point is – 2015 is going to be a year of increased regulation (and probably for the next several years ahead)

AMERICAN BANKER | Bank Technology News

Today's Paper | Magazine | Video | Web Seminars | White Papers | Women in Banking | FinTech F

DEALMAKING & STRATEGY | COMMUNITY BANKING | NATIONAL/ REGIONAL | LAW & REGULATION | CONSUMER FINANCE | BANK TECHNOLOGY | BANI

New York Attorney General Looks to Strengthen Data Security Laws

by EVAN NEMEROFF
JAN 16, 2015 3:44pm ET

New York Attorney General Eric Schneiderman is proposing legislation to strengthen data security laws to protect consumers from having their personal data stolen.

There currently is no law in New York that requires businesses to institute data security measures to protect consumer information. If a data breach occurs, companies only have to notify affected individuals if their "private information" was compromised.

RELATED

One Year After Target Breach, Consumers Vulnerable as Ever

Retail, Banking Trade Groups Form Cybersecurity Partnership

Almost Half U.S. Banks Are Reissuing Cards Due to Target Breach

The Biggest Data Breaches of the Year... (Gulp) So Far

Schneiderman's proposed bill would require business to notify a consumer if their email and passwords as well as security questions and answers were stolen in the event of a data breach or unauthorized disclosure. The definition of "private information" (for the purpose of notification) would also expand to include data about a consumer's medical information and health insurance. Currently, "private information" only pertains to protecting an individual's Social Security number, driver's license and credit card number. California has already implemented a similar rule.

Furthermore, all companies that collect "private information" should have security measures installed to protect this data. Schneiderman said this includes training employees to assess risks and instituting technical safeguards to identify threats within a business's network and respond to possible attacks. Businesses would have to obtain third-party audits and certifications annually confirming that they are complying with these data security requirements, Schneiderman said.

Let's start with healthcare regulation

- Currently, the 800 pound gorilla in the room
- First area of US privacy protection to go to such length and depth
- Significant monetary penalties
- Substantial enforcement resources
- Wasn't always the case
- The evolution of healthcare regulation is significant
- Demonstrates the road ahead for other areas of data privacy regulation that are not yet at HIPAA-level protections

HIPAA doesn't exist in a vacuum

- We tend to look at single industry solutions in US
- But privacy regulations do not exist in a vacuum
- Statutes/regulations build on each other
- HIPAA had many deficiencies
- But Congress learned from these inadequacies
- Stole a number of concepts from elsewhere and will be the source of corrective measures in other areas of privacy regulation
- Helps to understand the privacy/security industry in its entirety to see how these laws & regulations have evolved and will continue to evolve

Problem getting VERY serious – Part 1

- Right now the bad guys are winning and winning big
- 60 Minutes episode from Nov. 30, 2014
- Cybersecurity expert claims 97% of all businesses will have their systems breached in 2015
- What's the typical response
- Regulatory penalties, civil lawsuits, loss of reputation, loss of revenue
- E.g., Target is fending off at least 111 lawsuits from customers, banks and shareholders

Problem getting VERY serious – Part 2

- According to this article
- 90% of healthcare organizations have reported at least 1 data breach in the past 2 years
- More than 1/3 have reported MORE THAN FIVE!!!
- The URL for this story is: http://www.healthcareitnews.com/news/HIPAA-breach-response-tips-experts?topic=18,30

Healthcare IT News

Published in partnership with HIMSS

News Blog White Papers Webinars Jobs More

EHRs Meaningful Use Privacy & Security HIE ICD-10 Interoperability Mobile CPOE Policy

When insights create great outcomes.

Erin McCann, Associate Editor

Erin McCann is Associate Editor at *Healthcare IT News*. She covers healthcare privacy and security, meaningful use, ambulatory care and healthcare policy. Follow Erin on Twitter @EMcCannHITN and Google+

Breach response tips from experts

'Don't give in to individuals who want to sugar coat this.'

June 20, 2014

Tweet 12 +1 0 Recommend 6 Share 11

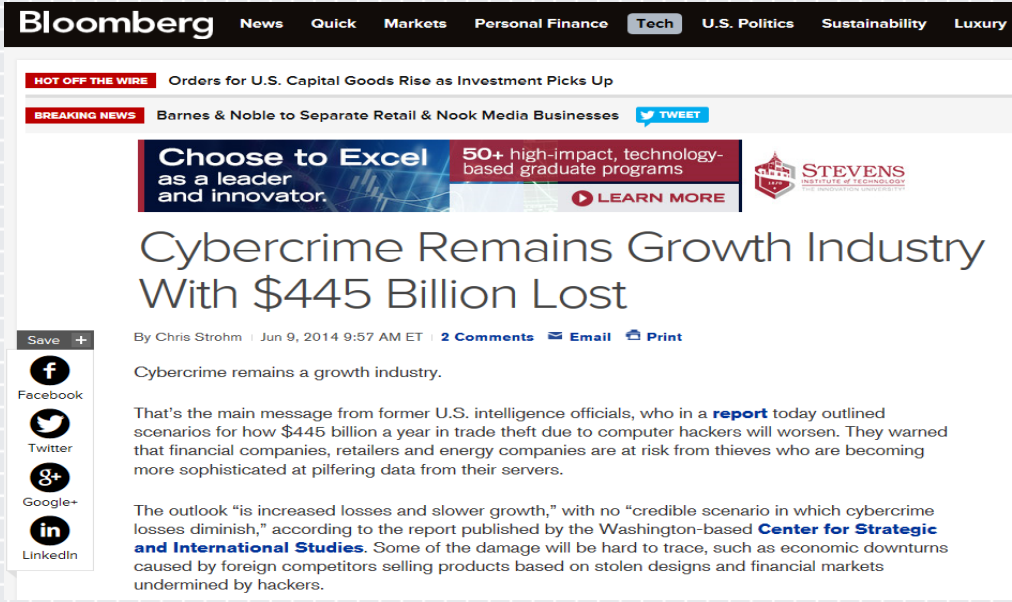
Some 90 percent of healthcare organizations have reported at least one data breach in the past two years, with more than a third seeing more than five breaches. Responding to these breaches in the proper manner proves integral not only to reining in costs and avoiding litigation but also to maintaining the integrity of the organization.

Gerry Hinkley, partner at Pillsbury Winthrop Shaw Pittman's healthcare practice, says breach response is where many make major missteps, mistakes that can easily be avoided.

Hinkley, who spoke at the HIMSS Media and *Healthcare IT News* Privacy and Security Forum June 16 in San Diego, works with myriad organizations on proper breach response, many of which have faced legal action due to post-breach slip-ups on their part. One of the biggest takeaways? "Don't give in to individuals who want to sugar coat this," he said. "You do much better really saying what happened up front ... individuals respect that."

Problem getting VERY serious – Part 3

- Title notes global $445 billion lost annually in trade theft & WILL WORSEN
- Taken from June, 2014 report of the Center for Strategic and International Studies
- The URL for the report is: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
- The URL for this story is: http://www.bloomberg.com/news/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost.html



Bloomberg News Quick Markets Personal Finance Tech U.S. Politics Sustainability Luxury

HOT OFF THE WIRE Orders for U.S. Capital Goods Rise as Investment Picks Up

BREAKING NEWS Barnes & Noble to Separate Retail & Nook Media Businesses TWEET

Cybercrime Remains Growth Industry With $445 Billion Lost

Save + Facebook Twitter Google+ LinkedIn

By Chris Strohm | Jun 9, 2014 9:57 AM ET | 2 Comments Email Print

Cybercrime remains a growth industry.

That's the main message from former U.S. intelligence officials, who in a **report** today outlined scenarios for how $445 billion a year in trade theft due to computer hackers will worsen. They warned that financial companies, retailers and energy companies are at risk from thieves who are becoming more sophisticated at pilfering data from their servers.

The outlook "is increased losses and slower growth," with no "credible scenario in which cybercrime losses diminish," according to the report published by the Washington-based **Center for Strategic and International Studies**. Some of the damage will be hard to trace, such as economic downturns caused by foreign competitors selling products based on stolen designs and financial markets undermined by hackers.

Sometime the problem is not knowing where data sits

- Affinity Health Plan from NY
- Leased 4 copiers
- Confidential ePHI was stored on copiers' hard drives
- Copiers returned to distributor at end of lease – no one thought to check the hard drives
- CBS Evening News bought one of the used hard drives & discovered the data
- Conducted an investigation & revealed the incident to Affinity who reported breach to HHS/OCR

$1.2 Million Penalty in Copier Breach

Affinity Health Plan, OCR Settle Over 2010 Incident

By Marianne Kolbasuk McGee, August 14, 2013.

Credit Eligible | Email | Tweet | Like | Share | Get Permission

Affinity

The latest **HIPAA** data breach settlement serves as a costly reminder that organizations must ensure they properly remove or destroy protected health information from all gear prior to disposal.

See Also: POS Security Essentials: How to Prevent Payment Card Breaches

Affinity Health Plan, a managed care plan company based in New York, has just agreed to pay federal regulators $1.2 million to settle a 2010 incident that affected 344,557 individuals whose data was discovered on the hard drives of copy machines that had been returned to a leasing company.

And while security experts say most organizations are more aware today than in 2010 about the data privacy and security risks posed by equipment such as copiers, printers, and fax machines, this settlement puts the risks in perspective.

"Someone forgets to sanitize the hard drive. The probability of this occurring these days, I would say is low," says independent security consultant Tom Walsh. "The impact if it happened would be high, as demonstrated by this breach by Affinity Health Plan and their OCR settlement."

Facts of the Case

At the center of the agreement was a **breach** reported by Affinity to the Department of Health and Human Services' Office for Civil Rights on April 15, 2010. Affinity discovered

RELATED CONTENT

- Cancer Center Breach Involves ID Theft
- ISACA Automates Cobit 5 Process
- Why Major Retailers Want Chip and PIN
- Fraud: Underground Markets Evolving
- Former NCUA Chair Outraged by Breach

RELATED WHITEPAPERS

- The Threat Landscape
- DMARC Guide: Understanding

“C-suite” getting worried?

- Good news/bad news
- CIOs under greater fire
- Target’s was fired
- Even Target’s CEO was asked to leave over this
- But events like these also justify bigger budgets
- To fend off cyber-attacks

abcNEWS HOME | VIDEO | U.S. | WORLD | POLITICS | ENTERTAINMENT | TECH

Target Breach Puts Corporate Tech Execs Under Fire

NEW YORK March 6, 2014 (AP)

By BREE FOWLER AP Technology Writer

AP

Hackers are putting top technology executives under severe pressure. And this week's sudden departure of Target's chief information officer in the wake of the company's massive pre-Christmas data breach has only ratcheted up the stress.

Years ago, the job of a CIO focused mainly on the upkeep of computer systems. In their largely behind-the-scenes roles, most of their major decisions centered on the kinds of technological innovations a company would adopt, when and how much to pay for systems upgrades and the creation and maintenance of company websites.

But the rise of computer crime in recent years changed the job description. At the same time, the surging use of personal smartphones and tablets in business settings has given CIOs even more technology to manage, along with countless new points of entry for hackers to breach their systems.

As a result, CIOs have their hands full and a much more high-profile role than ever before.

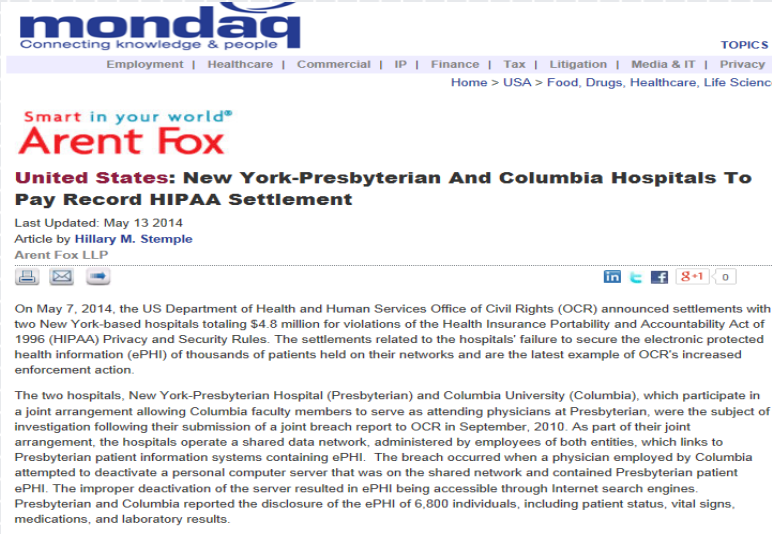
Target Corp.'s breach sent shockwaves through the profession. And CIOs from companies in all walks of business —from retail to banking and drug discovery— are using the breach as a rallying point to call attention to their struggle and garner additional funds and manpower to fight digital threats.

Cyberattacks were on the rise long before Target's news that hackers had stolen 40 million debit and credit card numbers, along with the personal information belonging to as many as 70,000 people. A 2013 Hewlett-Packard Co.-sponsored study by the Ponemon Institute found that the average annual cost of cybercrime incurred by a benchmark sample of U.S. organizations was $11.6 million per organization, a 26 percent increase from the previous year.

Largest US HIPAA assessment to date? May of 2014

$4.8 MILLION – NY Presbyterian & Columbia University Hospitals

- Joint settlement – largest US HIPAA penalty
- NY Pres allows Columbia docs to work there
- Columbia physician attempts to deactivate a personal computer on the hospital network
- Results in the inadvertent disclosure of 6800 Presbyterian Hospital patients' info on the Net
- Included patients' status, vital signs, meds & lab results
- $3.3 million for NY Presbyterian & 1.5 million for Columbia, plus corrective action plans which includes risk analysis and management plan, staff training, written policies and procedures creation



mondaq
Connecting knowledge & people

TOPICS

Employment | Healthcare | Commercial | IP | Finance | Tax | Litigation | Media & IT | Privacy

Home > USA > Food, Drugs, Healthcare, Life Scienc

Smart in your world®
Arent Fox

United States: New York-Presbyterian And Columbia Hospitals To Pay Record HIPAA Settlement

Last Updated: May 13 2014
Article by **Hillary M. Stemple**
Arent Fox LLP

On May 7, 2014, the US Department of Health and Human Services Office of Civil Rights (OCR) announced settlements with two New York-based hospitals totaling $4.8 million for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. The settlements related to the hospitals' failure to secure the electronic protected health information (ePHI) of thousands of patients held on their networks and are the latest example of OCR's increased enforcement action.

The two hospitals, New York-Presbyterian Hospital (Presbyterian) and Columbia University (Columbia), which participate in a joint arrangement allowing Columbia faculty members to serve as attending physicians at Presbyterian, were the subject of investigation following their submission of a joint breach report to OCR in September, 2010. As part of their joint arrangement, the hospitals operate a shared data network, administered by employees of both entities, which links to Presbyterian patient information systems containing ePHI. The breach occurred when a physician employed by Columbia attempted to deactivate a personal computer server that was on the shared network and contained Presbyterian patient ePHI. The improper deactivation of the server resulted in ePHI being accessible through Internet search engines. Presbyterian and Columbia reported the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

Biggest HIPAA assessment ANYWHERE

$6.8 MILLION HIT IN PUERTO RICO

- Medical insurer inadvertently released PHI
- Only 13,336 identities exposed in 2013
- Fine amounted to $500 per exposed identity
- Also got hit for $100,000 for not cooperating
- Ricardo Rivera Cardona, Director of the Puerto Rico Health Insurance Administration (ASES in Spanish) said it could have been much more

- His agency had the authority to fine up to $100,000 for every exposed identity
- Sharks smell blood – this insurer recently admitted to Absolute they've suffered over 80 audits in the past year

Why are privacy violations becoming more frequent (and expensive)?

ACCRETIVE HEALTH
results providers trust

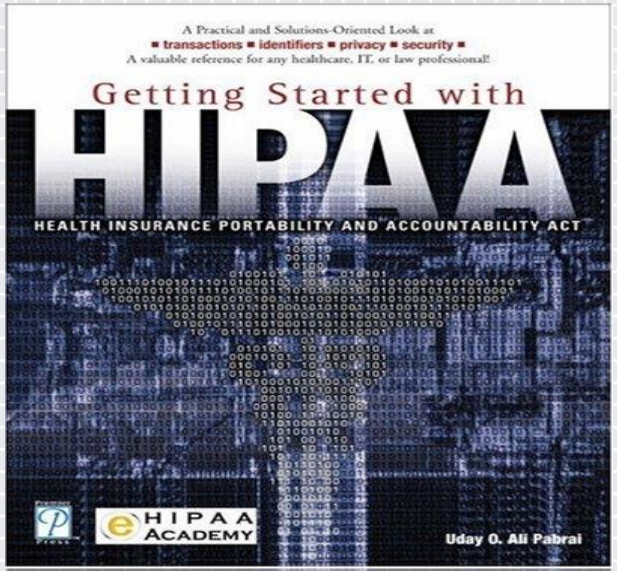
Minn. Attorney General Lori Swanson

- What happened to Accretive Health a perfect example
- HITECH Act authorized States' AGs to bring actions
- Accretive Business Associate to 2 Minnesota Hospitals
- Stolen unencrypted laptop contained personal healthcare info of 23,500 patients
- Condition of settlement – Accretive may not operate in Minnesota for AT LEAST 2 years beginning July, 2012
- Can be up to 6 years based on yearly review by Minnesota AG
- Estimated loss of revenue from Minnesota – $22-25 million per year
- Total current loss – over $70 million AND COUNTING

The toll on Accretive

Health Insurance and Portability Accountability Act (HIPAA) basics

- Created a “Privacy Rule”
- Can be found at: 45 Code of Federal Regulation (CFR) § 164.500 et.sec.
- Under the Privacy Rule, ALL forms of Protected Health Information (PHI) must be kept private (written, oral, digital, etc.)
- Created a “Security Rule”
- 45 CFR § 164.300 et.sec.
- Security Rule only requires electronic PHI (ePHI) be kept secure
- But as originally enacted in 1996 – a toothless tiger



What exactly is PHI?

- Info about a patient's past, present or future mental or physical health or any billing or payment
- Which can be connected to a specific patient
- By any one of 18 identifiers specified in the statute
- All your common identifiers
- But the 18th identifier leaves the possibilities completely open-ended

What changed so much with HIPAA?

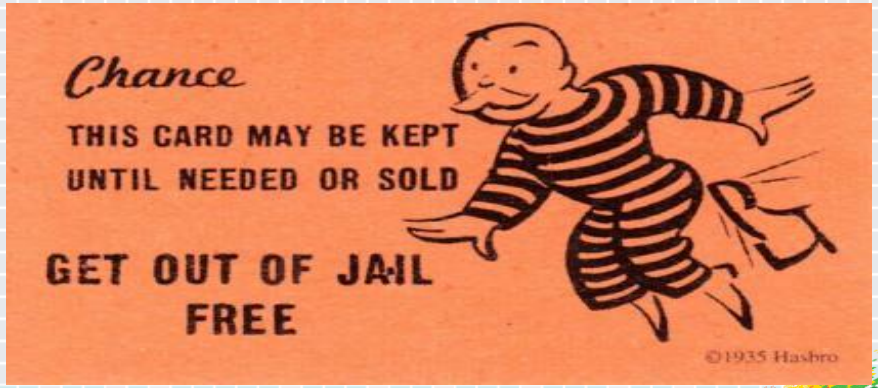
- Welcome to the Health Information Technology for Economic and Clinical Health Act – enacted in 2009
- Corrected many of the deficiencies of HIPAA – partly based on advances in other areas of privacy/security law
- Important move was to leave flexibility with HHS to enact modifying regulations with the creation of the Omnibus Final Rule which went into effect September 23, 2013

Overview of HITECH-OFR enhancements

- Many more entities now required to comply (not just “Covered Entities” but also “Business Associates and their subcontractors”)
- $ amount of civil penalties & fines GREATLY increased (from max of $50,000 per violation to $1.5 million per violation PER YEAR)
- Enforcement agencies now specified & numerous (State Attorneys Generals added to federal Department of Health & Human Services)
- Burden of proof shifted – data out of control of an authorized person is now *presumed* a breach, unless it can be shown there’s a “low probability protected data was lost”
- Created the Breach Notification Rule – 45 CFR § 164.400 et.sec.
- Entities now required to come forward with announcing breaches
- Mostly due to HITECH/OFR, enforcement & penalty $$ increased

One of the possible misconceptions if you only look at HITECH and not regs issued afterwards

- It gets said at HIPAA training sessions & by “C Suite” executives
- If you only read the HITECH Act, you could be led to believe that
- Be very, very careful here – just because someone says it so, doesn’t make it true
- Not aware of any court or administrative decision holding that way yet
- Must resort to reviewing statutory/regulatory language



When encryption is not enough?

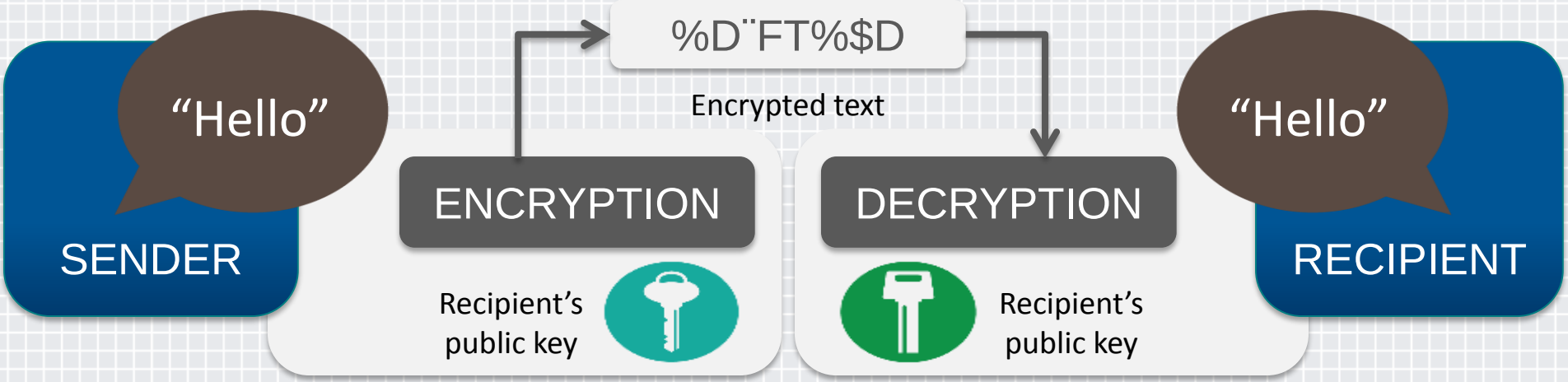
- Those who claim encryption is a safe harbor to HIPAA regulation should read 74 Federal Register 79 – issued 4/27/09
- Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- At page 19009 – "(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by 'the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key' and ***such confidential process or key that might enable decryption has not been breached.***"

B. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by ''the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key'' [15] and such confidential process or key that might enable decryption has not been breached.

What ways can encryption be decrypted?



- Brute force attack – very rare
- Sticky note on device – much more common
- Mistakenly granted administrative rights – disturbing way too common
- Device stolen by someone who knows the decryption key – also quite common

Expansion of entities covered by HIPAA / HITECH

Covered Entity

↓

Business Associate

↓

Subcontractor(s)

Liability & Satisfactory Assurances

↓

↑

Notification

- HIPAA applied only to “Covered Entities” – your basic healthcare providers
- One attempt to avoid HIPAA compliance was to pass duties off to 3rd parties
- HITECH & OFR extended compliance to “Business Associates” & their Subcontractors
- Covered Entities can potentially be financially liable for violations done by their downstream

What is a Business Associate?

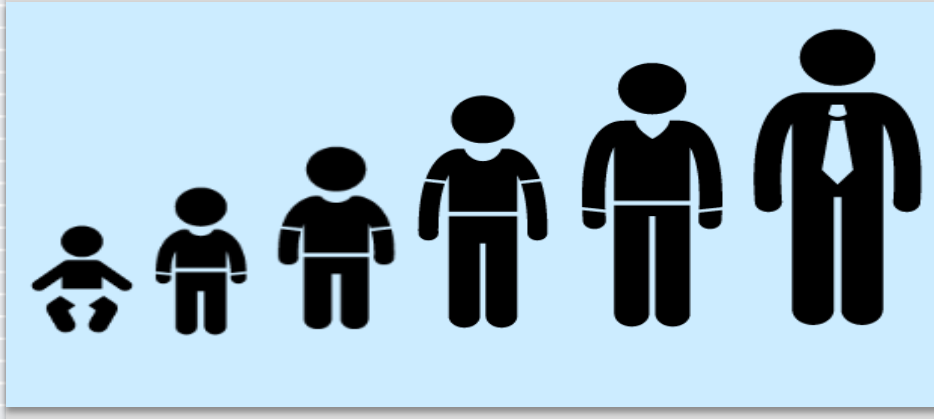
- No easy answer
- Guidance found in 45 CFR § 160.103
- Any organizations which "receive, create, maintain or transmit protected health information on behalf of a covered entity"
- “functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing”
- “services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial”
- A Covered Entity CAN be a Business Associate of another Covered Entity
- This mean once labeled a Covered Entity DOESN’T mean you’re always that
- So IMPORTANT query for Covered Entities – if YOU love a particular solution, and YOU’RE financially liable for the breaches of your downstream, why isn’t YOUR DOWNSTREAM required to use your solution?

Now a written relationship with Business Associate

- Not just liability flows downstream
- Business Associate & Covered Entity must have written agreement
- Can be a contract, can just be an agreement
- Written agreement must set forth BA's supervision of its subcontractors
- Supervision extends beyond simply having an agreement

What about other areas of privacy law?

- To make an evolutionary analogy here
- The post-HITECH era has quickly evolved HIPAA
- Moving from adolescence to adulthood
- For virtually all of the remaining areas of US law
- The stage of evolution is not nearly as advanced
- More like moving from toddler to childhood
- But remember, HIPAA evolved, in part, by learning from others
- One has to assume the others will also follow HIPAA
- Plus, we've already seen evidence of this



The other current big dog in the fight? The FTC

- 2006, ChoicePoint paid a fine of $10 mil to the FTC and a $5 mil fund for victims
- The data warehouser sold info from over 163,000 of its customers to an alleged crime ring
- Has used it authority under Section 5 of the FTC which prohibits unfair and deceptive acts or practices to reach over 50 settlements similar to the one in the Accretive Health case.
- The only area of compliance law/regulation currently under litigation in the US court system claim FTC lacks authority to do this
- 2 lower federal decisions have supported the FTC, one case recently affirmed by the respective Circuit Court of Appeal

The FTC is seeking to spread its wings

- It claims authority under the Gramm-Leach-Bliley Act to enact its own Security Rule to be enforced against non-banking financial institutions and demand privacy compliance

- In 2010, authority extended to health care providers not covered by HIPAA
- Also claims it is empowered by the Child Online Privacy Protection Act to require reasonable security for info collected only about children
- In Senate testimony in April, 2014, FTC Commissioner Edith Ramirez, requested federal legislation to strengthen its existing authority governing data security standards on companies, to impose civil penalties against violating companies and to mandate breach notification

What's ahead – A SLEW of US regulatory initiatives – the SEC

- Speech given by Luis A. Aguilar, SEC Commissioner on 6/10/14 at the NYSE
- "Cyber Risks and the Boardroom"
- Warning that SEC will become increasingly interested in how boards respond to cyber threats
- Boards MUST go beyond the minimum industry standards
- Must develop *proactive strategies*

U.S. Securities and Exchange Commission

Search SEC

ABOUT | DIVISIONS | ENFORCEMENT | REGULATION | EDUCATION | FILINGS | NEWS

Newsroom
Press Releases
Public Statements
Speeches
Testimony
Spotlight Topics
Media Kit
Events
Webcasts
What's New
Special Studies
RSS Feeds
Social Media

SPEECH

Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

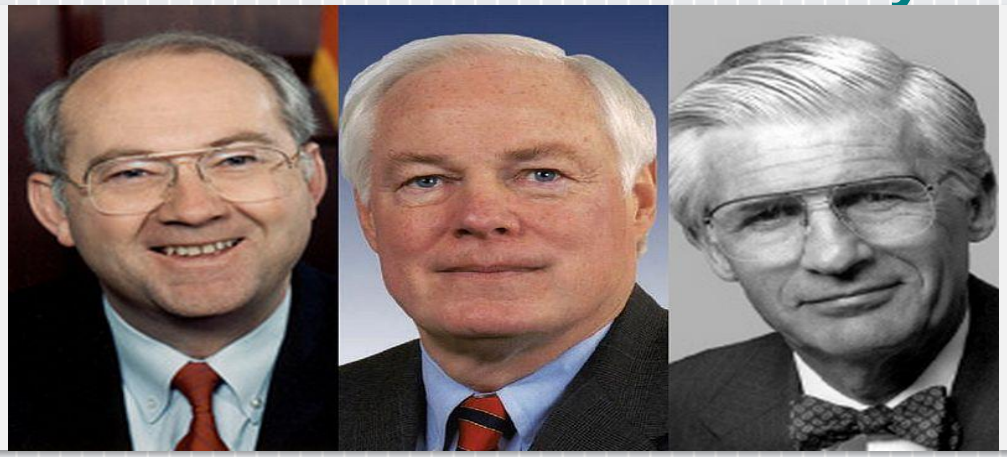
June 10, 2014

Good afternoon. Thank you for that kind introduction. I am glad to be back at the New York Stock Exchange. In anticipating today's conference, I thought back to an earlier trip to the NYSE where in April 2009, I had the opportunity to ring the closing bell. Before I begin my remarks, let me issue the standard disclaimer that the views I express today are my own, and do not necessarily reflect the views of the U.S. Securities and Exchange Commission ("SEC" or "Commission"), my fellow Commissioners, or members of the staff.

I am pleased to be here and to have the opportunity to speak about cyber-risks and the boardroom, a topic that is both timely and extremely important. Over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators.[1] I suspect that not too long ago, we would have been hard-pressed to find many individuals who had even heard of cybersecurity, let alone known what it meant. Yet, in the past few years, there can be no doubt that the focus on this issue has dramatically increased.[2]

Cybersecurity has become an important topic in both the private and public sectors, and for good reason. Law enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated.[3] Indeed, according to one survey, U.S. companies experienced a 42% increase between 2011 and 2012 in the number of successful cyber-attacks they experienced per week.[4] As I am sure you have heard, recently there have also been a series of well-publicized cyber-attacks that have generated considerable

Not just HIPAA – Gramm-Leach Bliley Act of 1999



- Has a “Privacy Rule” (PR) & “Safeguards Rule” (SR), 15 USC § § 6801-6809
- PR requires financial institutions to *report* to customers what info of theirs is *collected*, what info is *shared*, how it is *used*, how it is *protected*
- SR requires them to *designate an individual* to safeguard this data, do a *risk analysis* to insure it is safeguarded, *test* the procedures to safeguard the data and *change* it if necessary
- In 2003, the FTC added a *breach notification* requirement to GLB
- Has been used on the State level to support data protection compliance

Not just HIPAA – Sarbanes-Oxley Act of 2002 (SOX)

- Created to counter massive corporate fraud such as Enron and others
- Overwhelming Congressional response
- SOX § 302 – Disclosure provision to stockholders
- Criminal provision – 18 USC § 1350
- Civil provision – 15 USC § 7241
- Loss of Intellectual Property has been interpreted by think tanks as requiring SOX notification to stockholders
- http://www.thetso.com/Info/Executive%20Counsel%20Article.pdf
- Loss of personal info data should also require it

Not just HIPAA – State breach notification laws

- Slightly outdated diagram
- In 2014, Kentucky became 47th
- All 4 US territories have one
- Darker colors – tougher laws
- Virginia considered toughest penalties
- California started this with law effective 2003
- Instituted breach notification

- Generally applies to government agencies and businesses
- Some States' breach notification laws also cover healthcare

GLB's Security Rule applies to higher education institutions

- When they act as "financial institutions"
- E.g., when they keep records of student financial aid
- So claims the National Assn. of University and College Attorneys
- Claims the FTC has so ruled
- Check out their published analysis
- http://www.nacua.org/nacualert/docs/GLB_Note_051603i.html

What's ahead?

- Push for national breach notification law
- Earlier this year from the former US Attorney General
- Recently by President Obama in the press release in advance of his State of the Union address
- Spurred on by recent breaches at Target, Neiman Marcus, etc.
- Mandatory EHR/EMR by 2015
- Point is – no end in sight to private data going digital with regulations & statutes being created to protect

What's ahead – Random audits by the Federal Financial Institutions Examination Council

- Announced they will perform a HIPAA-style pilot inspection program in 2015
- Will audit 500 community banks
- Audits will focus on these same HIPAA-style issues
- Will include banks with under $10 billion in assets & limited purpose chartered institutions
- Threat intelligence & collaboration
- Cybersecurity controls
- Service provider & vendor risk management
- Cyber-incident management and resilience
- This mirrors PRECISELY what our contacts in the financial industry told us in spring of 2014

What's ahead

- EU data protection law undergoing major changes
- Data Protection Directive of 1995 to be amended
- Many concerns
- Obvious one is the Directive's age – many tech changes
- Also only advisory Directive
- Individual member states applied Directive differently

What's ahead

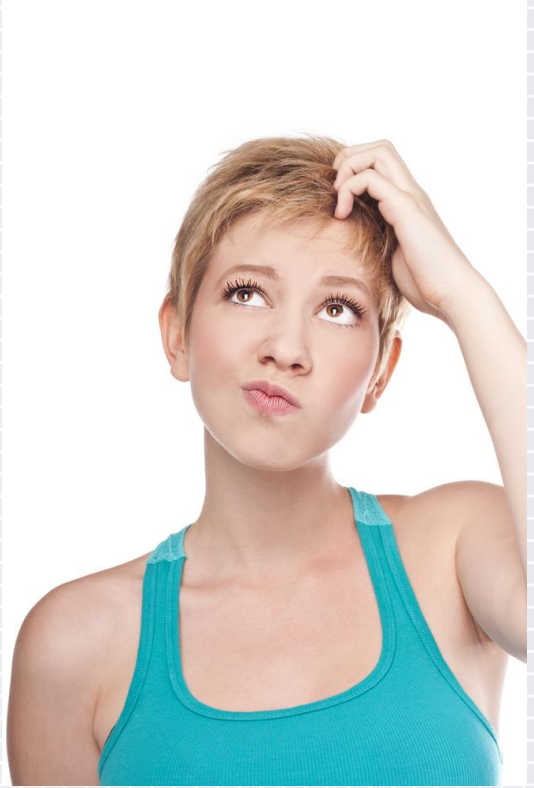
- EU Data Protection Regulation
- All 28 EU member states MUST adopt this once passed
- Applied not just to entities IN the EU but ANYONE DOING BUSINESS in the EU
- Adopts breach notification for the first time
- Institutes a statutory "Right to be Forgotten"
- 2%-5% global gross revenue penalty for violations

What's ahead – Court rulings

- Case law is starting to join the fray
- Civil suits use to be routinely dismissed
- Victim had to prove dollar lose reasonably attributed to breach
- Courts are starting to change that
- The potential for financial losses has been recently held as sufficient
- Another court penalized the breached company on the theory of the customer's subscription cost implied there'd be a secure data system
- An EU court found a "Right to be Forgotten" in the current Data Protection Directive

How to respond to these pressures/issues?

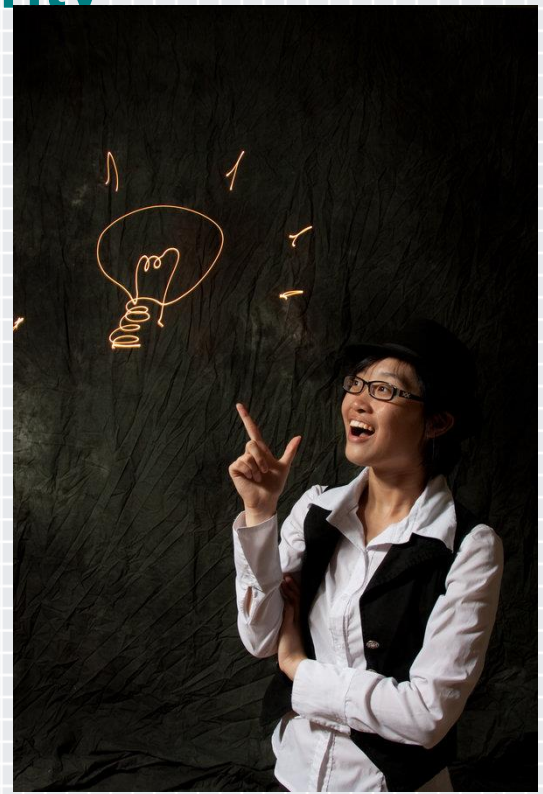
- Most of these you already know
- Multiple areas of risk
- Requires layered approach
- Policies/processes or procedures
- Employees BIG source of vulnerability
- Big stick/big carrot – applied equally to all
- No longer just guarding the gates, but hoarding off the invaders
- Limiting location of sensitive data
- Limiting ability to view accessed sensitive data (encryption)
- Being able to demonstrate all this (reports)



Data at risk resides in many places these days
Many devices, one solution, makes much sense

Some issues may not come to you immediately when it comes to mobile device security

- Can you remotely access device, device freeze, data delete
- Can remote access be interrupted by thief/unauthorized person
- Can remote access be assured – Think about Target's breach
- Can location of missing/stolen device be remotely tracked
- Can missing mobile device be recovered by law enforcement
- Must the victim of the loss/theft be the one to recover
- Can forensics be performed on recovered device
- Can encryption's existence during theft/loss be documented
- What about documenting access to sensitive data during theft/loss
- Being able to issue reports on all this



Any Questions?