Slide 1:

Sarbanes-Oxley, HIPAA and Privacy 101

Copyright © 2006 illustro Systems International, LLC

Slide 2:

Agenda

- Regulations, Regulations
  - "SOX"
  - HIPAA
  - GLBA
  - State of California
  - Others
- What motivated the regulations?
- Solutions and Best Practice – a primer

This is no way meant to be an exhaustive list of a way of ensuring you are compliant with any regulations. It's not even an exhaustive list of all the regulations, let alone how to be compliant. This is intended to be a primer on the concept, and we cannot even guarantee that it is an exhaustive primer. If any of these were true, we'd all be exhausted.

Copyright © 2006 illustro Systems International, LLC   WAVV2006-2

Slide 3:

Sarbanes-Oxley: a/k/a "SOX"

- Signed into law on July 30th, 2002
- Named after Senator Paul Sarbanes D-MD, and Representative Michael Oxley R-OH
- Introduced significant changes in financial reporting and mandates for publishing information

illustro Systems Inter   WAVV2006-3

SOX…

- Introduced a number of deadlines:
  - Most public companies must meet the financial reporting and certification mandates for any end of year financial statements filed after November 15th 2004 (amended from June 15th)
  - Smaller companies and foreign companies must meet these mandates for any statements filed after 15th July 2005 (amended from April 15th).

Copyright © 2006 illustro Systems International, LLC   WAVV2006-4

SOX…

- Introduced following a number of high profile corporate failures

Adelphia   **WORLDCOM**

ENRON

Copyright © 2006 illustro Systems International, LLC   WAVV2006-5

SOX…

- "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders"

Copyright © 2006 illustro Systems International, LLC   WAVV2006-6

SOX…

- Organized into 11 "titles"
- Section 404 causes the most concern because of rules governing public disclosure
  - Makes managers responsible for maintaining an "adequate internal control structure and procedures for financial reporting";
  - Demands that companies' auditors "attest" to the management's assessment of these controls and disclose any "material weaknesses"
  - Strong new criminal penalties await transgressors.
- Remarkable because of notoriety and media attention

The New York Times

Illustro
See The Light!
2006-7

Cost of SOX…

- According to a study published by one study from William E. Simon Graduate School of Business Administration at the University of Rochester the net private cost amounts to $1.4 trillion.
- Econometric estimate of "the loss in total market value around the most significant legislative events"—i.e., the costs minus the benefits as perceived by the stock market as the new rules were enacted.

Illustro
See The Light!
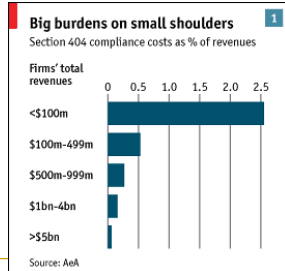Copyright © 2006 illustro Systems International, LLC
WAVV2006-8

Cost of SOX…

- Companies paid an average of $2.4m more for their most recent audits than anticipated
- Deloitte says large firms spent nearly 70,000 man hours complying with the new laws
- Bonanza for the "Final Four"
- Less visible costs, e.g. some companies are de-listing; foreign firms not listing

Illustro
See The Light!
Copyright © 2006 illustro Systems International, LLC
WAVV2006-9

Cost of SOX…

- Burden on smaller firms more dramatic

Big burdens on small shoulders
Section 404 compliance costs as % of revenues

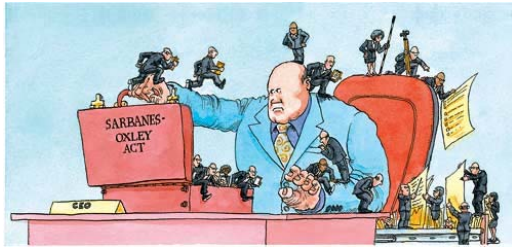| Firms' total revenues	0 0.5 1.0 1.5 2.0 2.5
<$100m	
$100m-499m	
$500m-999m	
$1bn-4bn	
>$5bn	

Source: AeA

Copyright © 2006 illustro Systems International, LLC   WAVV2006-10

Cost of SOX

Copyright © 2006 illustro Systems International, LLC   WAVV2006-11

SOX…

- High emphasis on financial reporting and corporate governance
- But implications for security, information protection and control management
- Security is a strong theme in SOX
- Most are modeling their responses on ISO17799
  - Very important standards related to information security

Copyright © 2006 illustro Systems International, LLC   WAVV2006-12

SOX...

3

HIPAA

- Not HIPPA (or Hippo!)
- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
- U.S. Department of HHS – enacted in 1996, initial deadline for providers – 2002
- Intended to improve Medicare process through standard transmission
  - This introduced privacy issues
- Who must comply (Covered Entities)?
  - Health Care Providers (who transmit electronic transactions covered by the HIPAA regulations)
  - Health Plans (self insured/insured, HMOs, health insurance companies, employer health plans, and similar arrangements)
  - Health Care Clearinghouses

Copyright © 2006 illustro Systems International, LLC   WAVV2006-14

HIPAA...

Copyright © 2006 illustro Systems International, LLC   WAVV2006-15

HIPAA – What It Mandates

- **Privacy** - provides new rules in regard to how an individual's health information may be used and disclosed by covered entities.
- **Transaction and Code Sets** - requires the use of standard transaction formats and code sets when an individual's financial health information is transmitted electronically by a covered entity for purposes of payment, coverage determinations, eligibility determinations, and similar business matters.
- **Security** - requires covered entities to have specific security measures in place to protect an individual's health information that is sent or stored electronically.
- Also carries civil and criminal penalties for non-compliance

Copyright © 2006 illustro Systems International, LLC   WAVV2006-16

HIPAA - Effects

Copyright © 2006 illustro Systems International, LLC   WAVV2006-17

HIPAA - Costs

- Estimates vary "slightly"
  - Overall costs to comply with HIPAA
    - $5.8 billion from the government agency in charge of the regulation
    - $43 billion from the Blue Cross-Blue Shield Association.
- Some analysts say it will cost more than Y2K conversion work

Copyright © 2006 illustro Systems International, LLC   WAVV2006-18

HIPAA - Costs

HIPAA Information Concerns

- Many software and hardware vendors promote the ability to achieve "HIPAA compliance"
  - Technology is only an enabler, cannot make compliant
- Requires:
  - Basic technology to adequately encrypt, authenticate or identify communication partners
  - Effective password-key management system when transmitting health-related information.
  - Reporting in the event of non-compliance
- Misconception that it bans some methods, e.g. PDAs and email

WAVV2006-20

GLBA

- The Gramm-Leach Bliley Act
- a/k/a The Financial Modernization Act of 1999
- Protect consumers personal financial information held by financial institutions

WAVV2006-21

GLBA…

- GLBA gives authority to 8 federal agencies and the states to enforce:
  - Financial Privacy Rule: governs the collection and disclosure of customers' personal financial information by financial institutions
  - The Safeguards Rule: requires all financial institutions to design, implement and maintain safeguards to protect customer information.

Copyright © 2006 illustro Systems International, LLC   WAVV2006-22

Some Others…

- FERPA - Family Educational Rights and Privacy Act
  - Parent's rights over students data
  - Rights transfer when student is 18
  - Cannot give parent information without student consent
- COPPA - Children's Online Privacy Protection Act
  - Give parents control over what information is collected from their children online and how such information may be used.

Copyright © 2006 illustro Systems International, LLC   WAVV2006-23

California – Privacy Legislation

- Any company that sells a product or service to a California resident, even if the company is based outside the state, may be affected.
- Just having a website that a California resident visits—and one out of 10 Americans lives in California—can put you under the jurisdiction of these laws.

Copyright © 2006 illustro Systems International, LLC   WAVV2006-24

California – Privacy Legislation…

- Identity theft driving the paranoia
  - Estimated 10 million Americans experienced I/T last year
  - Aberdeen group estimated losses could reach $2 trillion worldwide
- California passed SB 168
  - Prevented businesses from using SSN as identifiers
  - IBM last year required its more than 100 health insurance providers to stop printing Social Security numbers on medical ID cards, claims forms and other documents or risk losing their business
  - The change affected more than 540,000 IBM retirees, employees and their families in the United States

"But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed." - Shakespeare, Othello, act iii. Sc. 3.

Copyright © 2006 illustro Systems International, LLC   WAVV2006-25

Information, Information

- All regs are motivated by the same phenomena
  - Internet suddenly (literally) connected millions of heretofore separate systems
  - Vast quantity of information suddenly available
  - Common access (Web) and other methods made it relatively easy to obtain

Copyright © 2006 illustro Systems International, LLC

The Accepted was Suddenly Very, Very Bad

- Procedures that were de facto for decades were suddenly violations
  - Social Security Numbers as ID (military/schools/medical)
  - IT backup tapes sent off site
  - Even affected non-IT procedures
    - No more telephone information
    - Fax authorization forms

Copyright © 2006 illustro Systems International, LLC   WAVV2006-27

Fear – The Media Helps

Copyright © 2006 illustro Systems International, LLC   WAVV2006-28

Solutions?

- No quick fixes---in many cases these are long entrenched procedures, programs, and data stores that need to be adapted
- Awareness is the start of the equation
- Stretches to all facets of information handling, not just IT

Copyright © 2006 illustro Systems International, LLC   WAVV2006-29

Best Practices

- Most companies are either hiring or appointing a Chief Information Security Officer (CISO)
  - Mission is to safeguard the information (not technology) that the company has custody of
- First step is to educate all custodians of the legislation, the implications and the requirements

Copyright © 2006 illustro Systems International, LLC

Best Practices…

- Review and document information flow
  - Entry points and requirements, e.g.
    - Is Social Security Number Required for identification?
    - Is data sent over clear links on public networks?
  - Exit points and requirements, e.g.
    - Are required authorizations obtained before releasing information?
    - Are recipients authenticated adequately?
- Publish a Privacy Policy (Information handling)
- Monitor for breaches; if in doubt, NOTIFY

WAVV2006-31

Best Practices…

- From an IT perspective, many areas:
  - Consider ways of centralizing your data--- oh, wait, you're on a mainframe!!
  - Much easier to manage, audit, enact policies, control access
  - Others are seeing the "benefits" of centralized data and application control
  - www.citrix.com
  - Review backup policies, and actual results
    - Backups are NOT valid unless tested in restore

WAVV2006-32

Best Practices…

WAVV2006-33

Best Practices…

- Define and enforce access control policies through security software
  - Commercial security packages
  - Offer access and audit
  - For VSE – at least BSM and ACLR
- Explore ways to record session data
  - Can be used for triggers/alerts
  - Also for replay for audit, investigations
- Review encryption:
  - Needs
  - Wants
  - Budget

Best Practices…

Best Practices…

- Encryption has many possible "touchpoints"
  - Encrypted data at rest
  - Encrypted data at the field level for sensitive data, e.g. SSN
- Any data that leaves the confines of the physical and programmatic security data center should be encrypted
  - Offsite backup tape data
  - FTP data being transmitted ANYWHERE on public network
  - Screen traffic (Web, Telnet etc.)
  - Email data (Outlook has free encryption capability)
  - Instant Messenger Data
  - Print data (consider online print access only)
  - Laptop data
  - USB drive data

A "Healthy Paranoia"

- Abundance of inter-connectivity has brought us here
- Rethink tried-and-true processes
- Look for information "leakage"
- React wherever possible, but be sure to notify all appropriate
- Review, Respond, Repeat

A "Healthy Paranoia"

BOB'S DECISION NOT TO BE CONNECTED TO THE COMPUTER NETWORK CAUSED SOME SUSPICION ON THE PART OF THOSE WHO WERE.