



WAVV 2008
Chattanooga, TN

How Safe? Security, Audit and the Insider Threat





Copyright © 2008 illustro Systems International, LLC

Agenda

- Regulations, Regulations
 - U.S.
 - "SOX", HIPAA, GLBA
 - State of California, others
 - International
 - PCI-DSS, Basel2, MiFID
- What motivated the regulations?
- Insider threat
- 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. Certified under WAVV Regulation 2.079-SCC-2007

Copy of Presentation

→illustro.com/conferences



iBrowse




Copyright © 2008 illustro Systems International, LLC

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 InterWAVV2008-4

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 © 2008 illustro Systems International, LLCWAVV2008-5


SOX...

- Introduced following a number of high profile corporate failures





Copyright © 2008 illustro Systems International, LLCWAVV2008-6

SOX...



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




See The Light.


Copyright © 2008 illustro Systems International, LLC


WAVV2008-7

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


2008-8

See The Light.


Copyright © 2008 illustro Systems International, LLC

WAVV2008-8

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.


See The Light.

Copyright © 2008 illustro Systems International, LLC

WAVV2008-9

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



See The Light.™

Copyright © 2008 illustro Systems International, LLC

WAVV2008-10

Cost of SOX...

- Burden on smaller firms more dramatic



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

Firms' total revenues	Compliance costs as % of revenues
<\$100m	~2.4%
\$100m-499m	~1.2%
\$500m-999m	~0.8%
\$1bn-4bn	~0.4%
>\$5bn	~0.2%

Source: A&A





See The Light.™

Copyright © 2008 illustro Systems International, LLC

WAVV2008-11

Cost of SOX






See The Light.™


Copyright © 2008 illustro Systems International, LLC

WAVV2008-12

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

See The Light.


Copyright © 2008 illustro Systems International, LLC


WAVV2008-13

SOX...



http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley





See The Light.


Copyright © 2008 illustro Systems International, LLC

WAVV2008-14

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

See The Light.

Copyright © 2008 illustro Systems International, LLC

WAVV2008-15

HIPAA...

<http://www.hipaadvisory.com/tech/>

iBrowse

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

HIPAA - Effects


<http://www.upmc.com/Hospitals/Facilities/Magee/IntheNews/Articles/NessHIPAAJAMA.htm>

iBrowse

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 © 2008 illustro Systems International, LLC

WAVV2008-19

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



Copyright © 2008 illustro Systems International, LLC

WAVV2008-20

GLBA






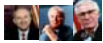
- The Gramm-Leach Bliley Act
- a/k/a The Financial Modernization Act of 1999
- Protect consumers personal financial information held by financial institutions




Copyright © 2008 illustro Systems International, LLC

WAVV2008-21

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.





See The Light.™


Copyright © 2008 illustro Systems International, LLC

WAVV2008-22

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.





See The Light.™


Copyright © 2008 illustro Systems International, LLC

WAVV2008-23

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.



See The Light.™

Copyright © 2008 illustro Systems International, LLC


WAVV2008-24

California – Privacy Legislation..

- Identity theft driving the paranoia
 - Estimated 24 million Americans experienced I/T in 2007
 - Aberdeen group estimated losses could reach \$2 trillion worldwide
- California passed SB 168
 - Prevented businesses from using SSN as identifiers
 - IBM recently 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.

illustro
See The Light.
Copyright © 2008 illustro Systems International, LLC WAVV2008-25



PCI - DSS

- **Payment Card Industry – Data Security Standards**
 - Developed by major credit card companies
 - Guideline to help companies prevent fraud, hacking and other issues
 - Any company which processes, stores or transmits credit card numbers must be PCI-DSS compliant


illustro
See The Light.
Copyright © 2008 illustro Systems International, LLC



PCI – DSS...

- Originally began as 5 different programs
 - VISA Information Security Program
 - MasterCard Site Data Protection
 - American Express Data Security Operating Policy
 - Discover Information and Compliance
 - JCB Data Security Program
- 15 December 2004 common causes aligned their policies and published PCI-DSS
- September 2006 standard was updated to 1.1

illustro
See The Light.
Copyright © 2008 illustro Systems International, LLC



PCI – DSS...

The control objectives and their requirements are:

- Build and Maintain a Secure Network
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 - Requirement 3: **Protect stored cardholder data**
 - Requirement 4: **Encrypt transmission of cardholder data across open, public networks**
- Maintain a Vulnerability Management Program
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: **Develop and maintain secure systems and applications**
- Implement Strong Access Control Measures
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
 - Requirement 10: **Track and monitor all access to network resources and cardholder data**
 - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
 - Requirement 12: Maintain a policy that addresses information security



Copyright © 2008 illustro Systems International, LLC

Basel II

- Second accord of the Basel Committee on Banking Supervision- members of G10
- Purpose is to create an international standard that banking regulators can use when creating regulations about risks bank face
- Aimed at the banking industry
 - Architected under a “3 Pillar Concept”
 - (1) minimum capital requirements (addressing risk),
 - (2) **supervisory review – guard against internal and external fraud**
 - (3) market discipline – to promote greater stability in the financial system.



Copyright © 2008 illustro Systems International, LLC

WAVV2008-29

MiFID


- **Markets in Financial Instruments Directive**
 - Introduces a single regulatory regime for investment services across the European Economic Area (27 member states + Iceland, Norway and Lichtenstein)
 - Cornerstone of European Commission's Financial Services Action Plan
 - 3 Objectives
 - To complete the process of creating a single EU market for investment services
 - To respond to changes and innovations which have occurred in securities markets
 - **To protect investors by making markets deeper, more competitive and more robust against fraud and abuse**




Copyright © 2008 illustro Systems International, LLC

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 © 2008 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
 - All "insiders" (employees, internal users) were doing what they were supposed to
 - Even affected non-IT procedures
 - No more telephone information
 - Fax authorization forms



Copyright © 2008 illustro Systems International, LLC

Fear




The State Department has sent the passport files of Sen. Barack Obama, left, Sen. John McCain, center, and Sen. Hillary Clinton, right, were promptly searched. State Dept. has committed to full disclosure for "a full investigation."

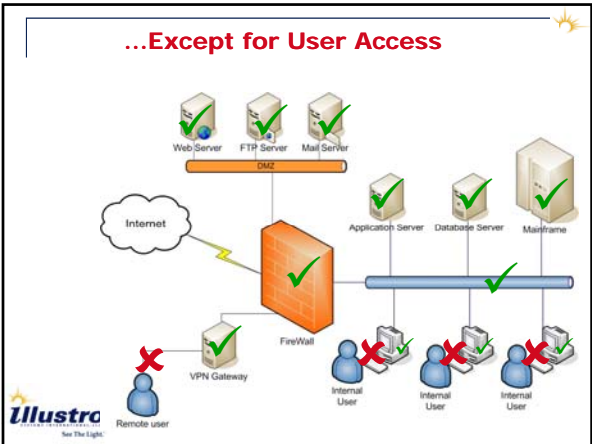
AP photos

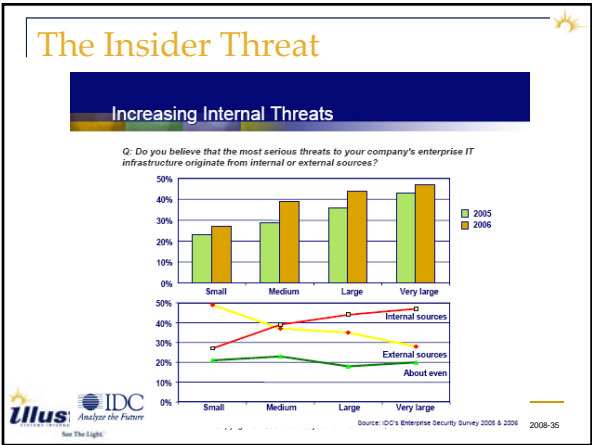
State Dept. investigating passport-data snooping
By Emily Bazelon and Marshall Hoels, USA TODAY

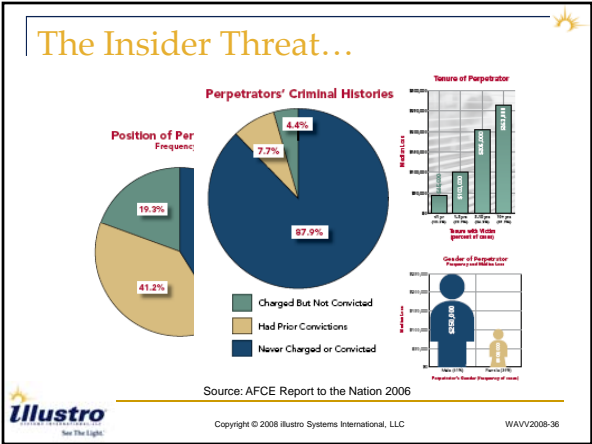
The passport files of presidential candidates Hillary Clinton and John McCain were reportedly searched by State Dept. officials.




Copyright © 2008 illustro Systems International, LLC










The Insider Threat


- The ACFE 2006 survey (Association of Certified Fraud Examiners)
 - Average Cost of Fraud - 5% of annual revenues
 - 60% of all frauds involves the employees
 - 60% of frauds are detected by tipping or by accident
 - The average scheme goes on for 18 months prior to detection



See The Light.


Copyright © 2008 illustro Systems International, LLC

WAVV2008-37



The Insider Threat...

- The FDIC 2004 Report (Federal Deposit Insurance Corporation)
 - 65%-70% of identity theft cases are committed with confidential information stolen by insiders
- Ernst & Young 2004 Security Survey
 - "The fact that internal incidents don't garner media coverage isn't because they don't happen...they simply are not made public, or even worse, undetected"



See The Light.

Copyright © 2008 illustro Systems International, LLC

WAVV2008-38



YOUR NEWEST HOT SHOT RECRUITS MIGHT BE DOING ALL THE WRONG THINGS... BEHIND YOUR BACK.

STOP POTENTIAL LEGAL MATTERS - TRACK INTERNAL DATA ACCESS.
Control and intelligent records are vital to help you to help you in your competitive industry, but don't allow those threats to destroy the integrity of your business.

That's where illustro's **Know** System comes in. **Know** is a powerful "behind-the-scenes" system. The **Know** system allows you to capture every single screen passing through your system so you can monitor any unauthorized access of company data. Once data is captured and recorded, it's available to you in a secure, searchable database. You can also establish a **proactive environment** which notifies you of specific events. Then you can decide if it's being viewed or used correctly.

Know What's Happening? Keep an eye on who's using your data. Call (888) 4-illustro or visit www.illustro.com/known today.





EVEN THOUGH YOUR TOP EMPLOYEES HAVE YOUR AUTHORIZATION TO VIEW PERSONAL DATA, THEY MAY BE USING IT AGAINST YOU.

REGULATIONS COMPLIANCE CAN BE (BYPASSED) BY INTERNAL THREAT.
Behind every bank, potential disaster event. Compliance with regulations and privacy legislation, including Sarbanes-Oxley, HIPAA and GLBA should have you more than just concerned... you should be terrified.

The **Know** system from illustro (**Know** System) is a powerful "behind-the-scenes" system. The **Know** system allows you to capture every single screen passing through your system so you can monitor any unauthorized access of company data. Once data is captured and recorded, it's available to you in a secure, searchable database. You can also establish a **proactive environment** which notifies you of specific events. Then you can decide if it's being viewed or used correctly.

Know What's Happening? Put an eye on who's using your data. Call (888) 4-illustro or visit www.illustro.com/known today.



Insider Threat in Banking & Finance

- *US Secret Service research (6/2005)*
 - Most incidents studied required little technical sophistication
 - In 87% of the cases studied, the insiders employed simple, legitimate user commands to carry out the incidents
 - In 78% of the incidents, the insiders were authorized users with active computer accounts at the time of the incident
 - Only 23% of the insiders were employed in technical positions, with 17% of the insiders possessing system administrator/root access within the organization
 - In 74% of the cases, after detection, the insiders' identities were obtained using system logs



Copyright © 2008 illustro Systems International, LLC WAVV2008-40

The Audit Trail Challenge

- The Fact - Many organizations have logs of update actions only, excluding queries
 - The problem - Not Sufficient for Privacy Protection regulations
- The Challenge – Include all user actions in the log
 - Sufficient for privacy regulations compliance as well as fraud detection



Copyright © 2008 illustro Systems International, LLC WAVV2008-41

The Challenge of Securing Legacy Systems

- Legacy systems typically do not have the controls required by today's regulations
- Adding controls to legacy systems requires knowledge & resources sometimes not available
- The result: Legacy systems may cause operational risk and non-compliance
- The solution: Compensating Controls can be deployed by External monitoring



Copyright © 2008 illustro Systems International, LLC WAVV2008-42

Existing Fraud Detection Solutions

- Analyze data stores - limited tracking of end-user actions and only after the fact
- Analyze system output (transactions, emails, etc.) – analyze traceable outputs only
- Visibility into end user actions requires intervention in thousands of application programs
- Bottom Line
 - No visibility into end-user actions,
 - especially queries and other actions that do not leave traces in the systems databases and outputs



Copyright © 2008 illustro Systems International, LLC

WAVV2008-43



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 © 2008 illustro Systems International, LLC

WAVV2008-44

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 © 2008 illustro Systems International, LLC


WAVV2008-45



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




Copyright © 2008 illustro Systems International, LLC

WAVV2008-46

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



Copyright © 2008 illustro Systems International, LLC

WAVV2008-47

Best Practices...





WAVV2008-48

Best Practices...

- Define and enforce access control policies through security software
 - Commercial security packages
 - 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
 - Record every screen *accessed*, whether changed or not
- Review encryption:
 - Needs
 - Wants
 - Budget




See The Light.™

Copyright © 2008 illustro Systems International, LLC

WAVV2008-49

Best Practices...

- Encryption has many possible “touchpoints”
 - Encrypted data at rest
 - Encrypted data at the field level for sensitive data, e.g. SSN
 - Encrypted data over the wire (e.g. SSL)
- 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




See The Light.™


Copyright © 2008 illustro Systems International, LLC

WAVV2008-50

A “Healthy Paranoia”



- Abundant activity has brought to light
- Rethink traditional processes
- Look for information “leakage”
- React when necessary but be sure to notify all appropriate
- Review, Respond, Repeat



See The Light.™

Copyright © 2008 illustro Systems International, LLC

WAVV2008-51

