


SDForum Security SIG
Palo Alto, CA
July 24, 2008

Understanding the Insider Threat in IT



illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

Copy of Presentation → illustro.com/presentations

iBrowse

illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

SDForum-2

Agenda

- Who is illustro
- The proliferation of information
- The Insider Threat – Do You Know?
- 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 SDForum Regulation 2.678-SCC.2007

illustro Systems International, LLC...

- Privately held firm based in Dallas, Texas
- Focus is on bridging the gaps for Enterprise data centers
- Network of partnerships
 - IBM Business Partner
 - IntellinX
 - International sales partnerships
- Customers across all industries depend on illustro





illustro Corporate Headquarters at the
Infomart—Dallas, Texas



Copyright © 2008 illustro Systems International, LLC

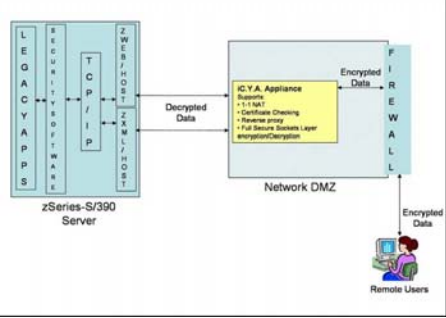
SDForum-4





Network Security

- Complete, turnkey solution — delivered completely ready to use
- Works with any TCP/IP Stack,
- Works for HTTP (Web), FTP, Telnet and other applications
- Supports SSL 3.0 and TLS 1.0
- Supports encryption algorithms including Triple DES, DES, both AES 128-bit and 256-bit
- RSA certified public/private encryption
- Supports most 3rd Party SSL Certificates (Verisign, etc.)
- Supports self-signed certificates
- Audit log Redundant hardware for maximum reliability
- Dual embedded 10/100/Gigabit NICs – Token-Ring capable
- Live demo available at www.illustro.com/icya.htm






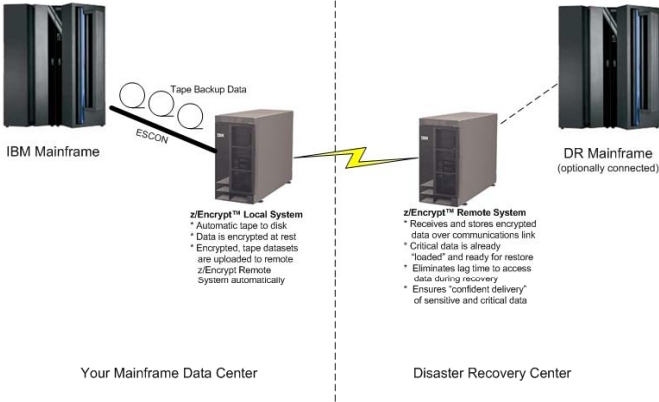
Copyright © 2008 illustro Systems International, LLC



Product Description




Mainframe Backup Protection




Your Mainframe Data Center

Disaster Recovery Center



Copyright © 2008 illustro Systems International, LLC



Product Description

Information, Information

- And now, a plethora of regulations to comply with, e.g. SOX/GLBA/HIPAA
- 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


SDForum-10



The screenshot shows the USA Today website with a navigation bar at the top. The main headline is "State Dept. investigating passport-data snooping" by Emily Bazar and Marisol Bello, USA TODAY. The article text states: "The State Department has said the passport files of Sen. Barack Obama, left; Sen. John McCain, center; and Sen. Hillary Clinton, right, were improperly breached. State Dept. Sec. Condoleezza Rice has called for 'a full investigation.'" Below the headline is a photo of Secretary of State Condoleezza Rice. The article is dated "Updated 30d ago" and has 1,161 comments and 56 recommendations. The page footer includes the copyright notice "Copyright © 2008 illustro Systems International, LLC" and the identifier "SDForum-11".




The screenshot shows a presentation slide titled "The Insider Threat". The slide is mostly blank, with a large rectangular area in the center. The word "iBrowse" is visible in the center of this area. The slide footer includes the copyright notice "Copyright © 2008 illustro Systems International, LLC" and the identifier "SDForum-12".




2006 REPORT TO THE NATION ON OCCUPATIONAL FRAUD & ABUSE

- **Occupational fraud and abuse imposes enormous costs on organizations.** The median loss caused by the occupational frauds in this study was \$159,000. Nearly one-quarter of the cases caused at least \$1 million in losses and nine cases caused losses of \$1 billion or more.
- Participants in our study estimate U.S. organizations lose 5% of their annual revenues to fraud. Applied to the estimated 2006 United States Gross Domestic Product, **this 5% figure would translate to approximately \$652 billion in fraud losses.** In 2004, participants estimated 6% of revenue was lost to fraud.
- **Occupational fraud schemes can be very difficult to detect.** The median length of the schemes in our study was 18 months from the time the fraud began until the time it was detected.



Copyright © 2008 illustro Systems International, LLC SDForum-13




2006 REPORT TO THE NATION ON OCCUPATIONAL FRAUD & ABUSE

Industry	# Cases	% Cases	Med. Loss
Banking/Financial Services	148	14.3%	\$258,000
Government and Public Administration	119	11.5%	\$82,000
Manufacturing	101	9.7%	\$413,000
Health Care	89	8.6%	\$160,000
Insurance	78	7.5%	\$100,000
Retail	75	7.2%	\$80,000
Education	73	7.0%	\$100,000
Service (general)	60	5.8%	\$163,000
Service (professional, scientific or technical)	58	5.6%	\$300,000
Construction	35	3.4%	\$500,000
Utilities	34	3.3%	\$124,000
Oil and Gas	32	3.1%	\$154,000
Real Estate	30	2.9%	\$200,000
Wholesale Trade	30	2.9%	\$1,000,000
Transportation and Warehousing	27	2.6%	\$109,000
Arts, Entertainment and Recreation	22	2.1%	\$175,000
Communications/Publishing	16	1.5%	\$225,000
Agriculture, Forestry, Fishing and Hunting	8	0.8%	\$71,000
Mining	1	0.1%	\$17,000,000

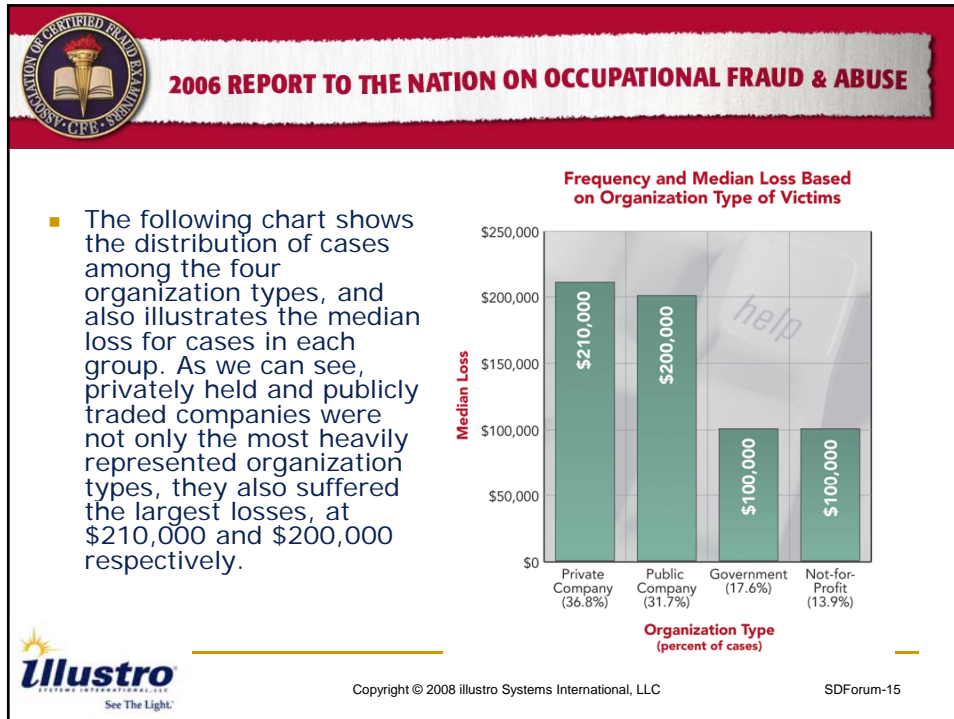
Excluding mining, which only had one case (costing \$17 million), the highest losses occurred in the wholesale trade industry, which had a median loss of \$1 million among 30 cases.

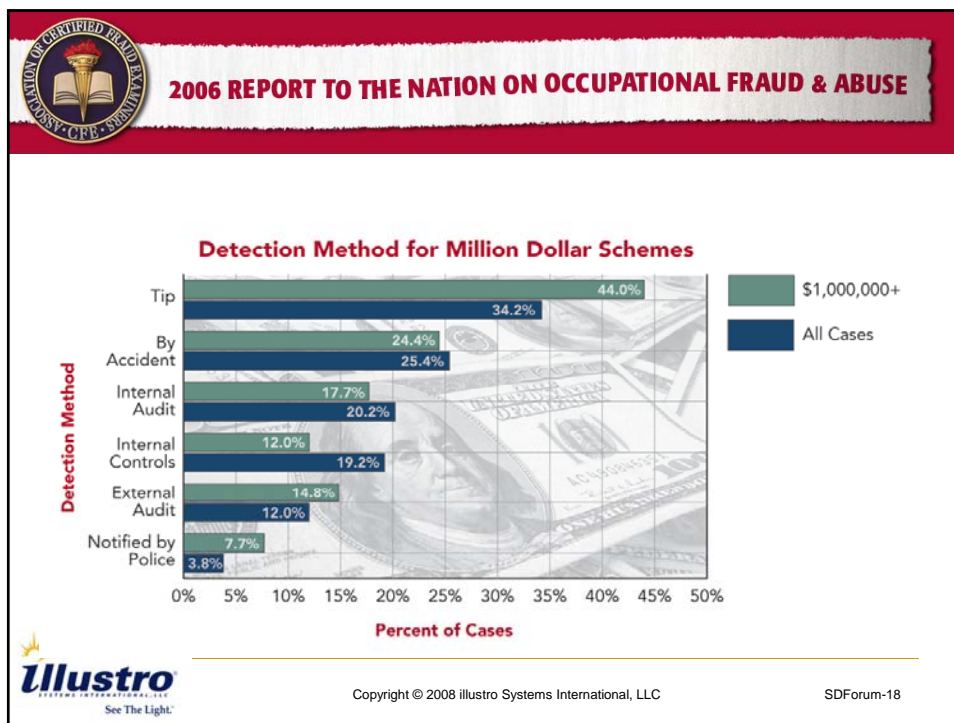
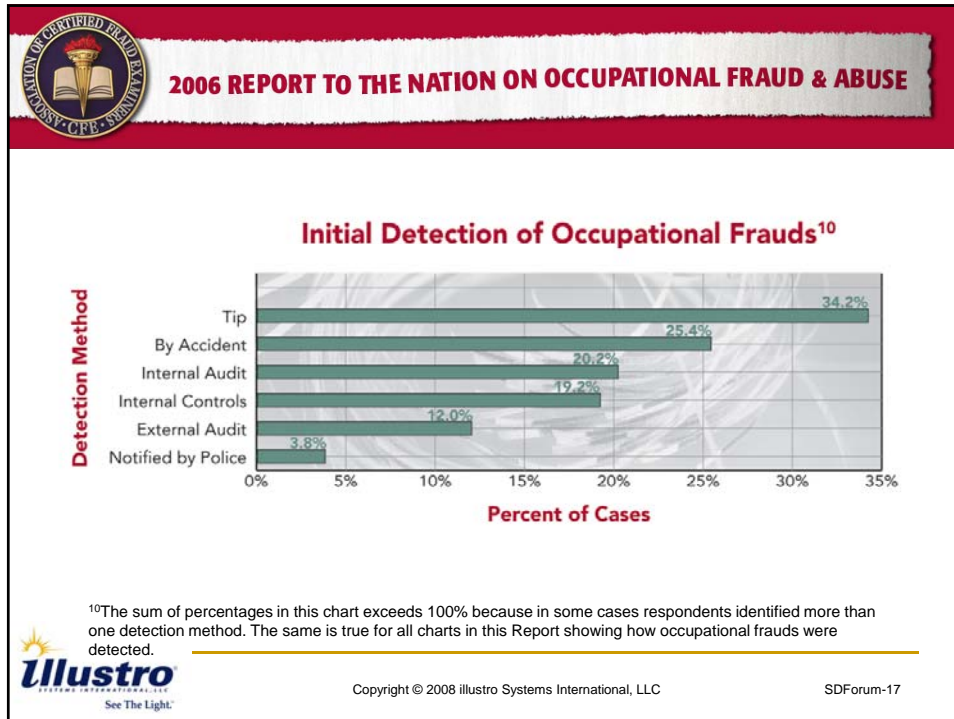
Next highest were construction, with a median loss of \$500,000 among 35 cases, and manufacturing, with a median loss of \$413,000 among 101 cases.

Among the industries that showed the lowest median losses were retail (median loss of \$80,000 among 75 cases) and government and public administration (median loss of \$82,000 among 110 cases).



Copyright © 2008 illustro Systems International, LLC SDForum-14





The Perpetrators



The perpetrators of occupational fraud are the people who use their positions within an organization for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

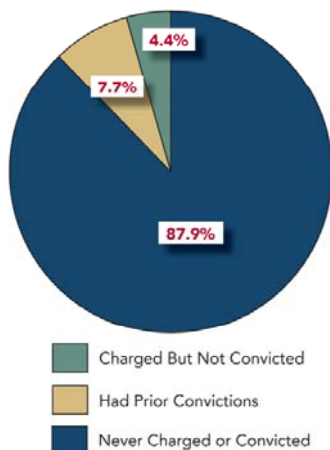


Copyright © 2008 illustro Systems International, LLC

SDForum-19

The Perpetrators...

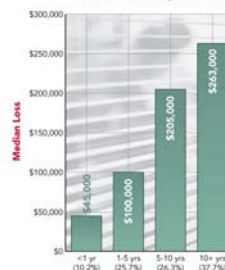
Perpetrators' Criminal Histories



Source: ACFE Report to the Nation 2006

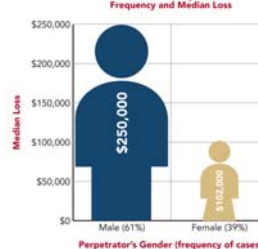
Copyright © 2008 illustro Systems International, LLC

Tenure of Perpetrator



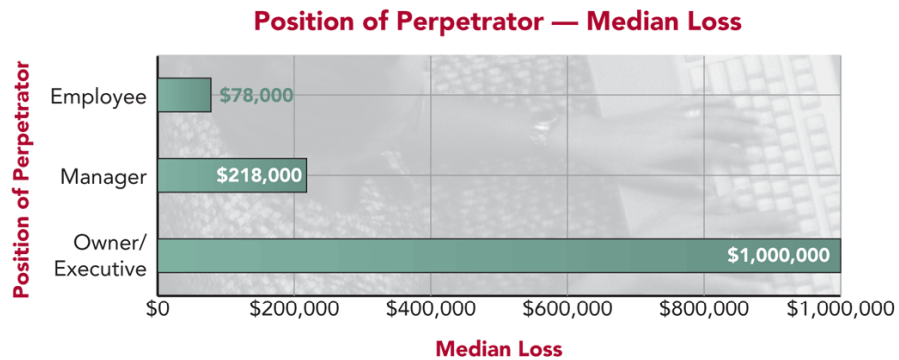
Tenure with Victim (percent of cases)

Gender of Perpetrator



Perpetrator's Gender (frequency of cases)

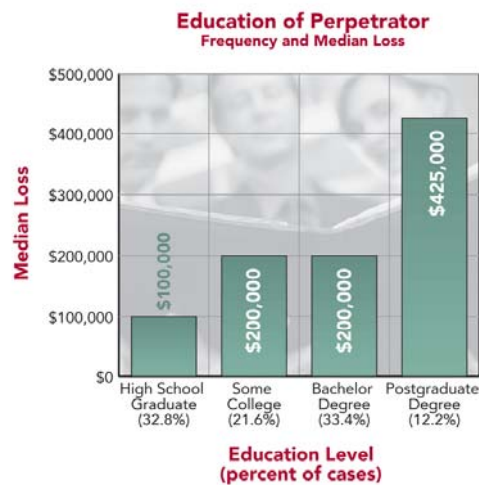
The Perpetrators...



Source: ACFE Report to the Nation 2006

Copyright © 2008 illustro Systems International, LLC

The Perpetrators...



Source: ACFE Report to the Nation 2006

Copyright © 2008 illustro Systems International, LLC

Why Don't We Hear More?

- "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, remain undetected"

Ernst & Young Security Survey

- In 78% of the incidents, the insiders were authorized users utilizing Simple, legitimate user commands

The US Secret Service research (June 2005)

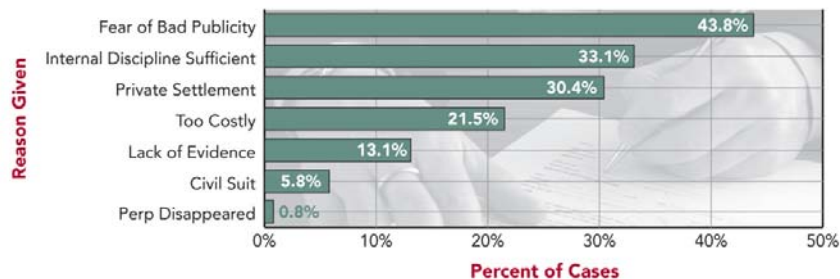


Copyright © 2008 illustro Systems International, LLC

SDForum-23

Keeping it Quiet

Reasons for Declining to Prosecute¹⁴



Source: ACFE Report to the Nation 2006

Copyright © 2008 illustro Systems International, LLC

SDForum-24

Real Cases: Employee Fraud

- **Capital Financial – March 2006**
26 customers lost 328,000 Pounds; fined for having poor anti-fraud controls – 300,000 pounds.
- **BNP Paribas Private Bank – May 2007**
Fraudulent transfer of 1.4 million pounds out of clients' accounts without permission; fined 350,000 pounds for weaknesses in systems and controls
- **Commerce Bancorp – November 2007**
Employee leaked confidential customer information



Copyright © 2008 illustro Systems International, LLC

SDForum-25

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

SDForum-26

The Audit Trail Challenge

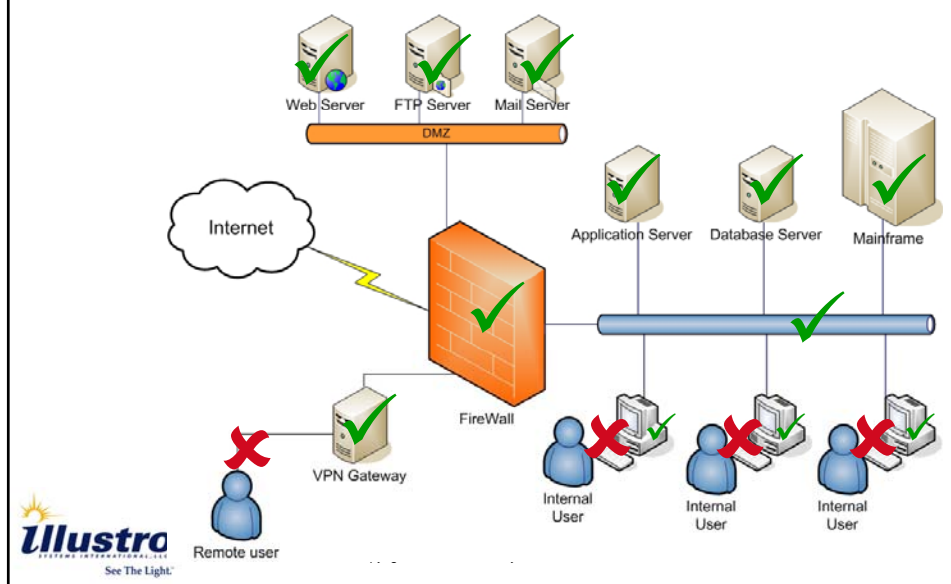
- The Fact - Many organizations have logs of update actions only, excluding queries
 - The problem - Not Sufficient for Privacy Protection regulations
- The Challenge – Include all user actions in the log
 - Sufficient for privacy regulations compliance as well as fraud detection



Copyright © 2008 illustro Systems International, LLC

SDForum-27

...Except for User Access



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



SDForum-29

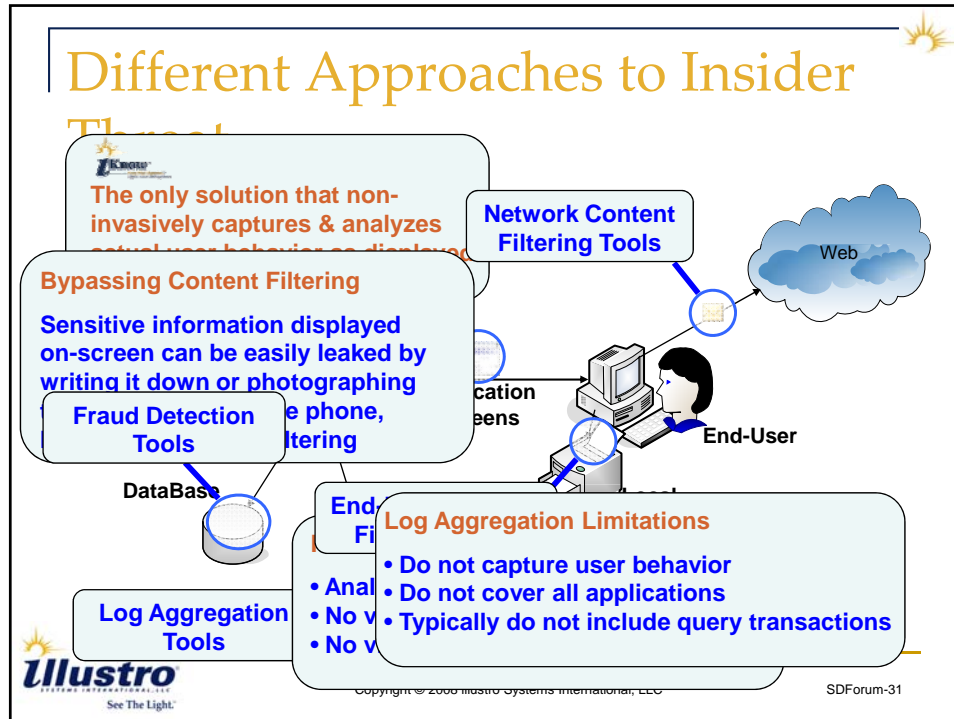
Solutions?

- 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

SDForum-30



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

STOP POTENTIAL LEGAL MATTERS - TRACK INTERNAL DATA ACCESS.

Curious and intelligent minds are traits you look for in new hires to help you in your competitive industry, but don't allow those attributes to **destroy the integrity of your business.**

That's where illustro's iKnow™ System Access Audit Appliance using IntelliX™ technology delivers. The iKnow appliance allows you to **capture every single screen passing through your system** so you can **monitor any unauthorized access or use of company data.** Since every screen and keystroke is recorded, you can setup a passive recording capability to **satisfy audit requirements**, even **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 eyeing your data.
Call (866) 4-illustro or visit illustro.com/eye today.

illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

© Copyright © 2008 illustro Systems International, LLC. All Rights Reserved. All trademarks referenced herein are trademarks of their original companies. iKnow, iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC.

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

REGULATIONS COMPLIANCE CAN BE JEOPARDIZED BY INTERNAL THREAT.


Behind every smile, potential disaster awaits. Compliance with regulations and privacy legislation including Sarbanes-Oxley, HIPAA and GLBA should have you more than just concerned...you should be **terrified.**

The terror stops here. With illustro's iKnow™ System Access Audit Appliance using IntelliX™ technology, every mainframe, AS/400 or Web screen passing through your network is captured and archived to a fully queryable database. Every screen and keystroke is recorded, allowing you to decide if it's being viewed or used correctly.

Know What's Happening™ - Put an end to internal threat.
Call (866) 4-illustro or visit illustro.com/threat today.

illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

© Copyright © 2008 illustro Systems International, LLC. All Rights Reserved. All trademarks referenced herein are trademarks of their original companies. iKnow, iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC. iKnow 3.0, and iKnow 3.0+ are trademarks of illustro Systems International, LLC.



I Know™

Know What's Happening™
System Access Audit Appliance


System Access Audit Appliance


Record and Replay - Corporate "BLACK BOX"

- Record **all** end user interaction with back office systems
- Replay **complete** user sessions
- "Google like" search on screen content

Analytics Engine

- Real time rules track user behavior patterns and detect internal fraud
- New rules may be applied after-the-fact to pre-recorded data






Illustruro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

SDForum-33




I Know™

Know What's Happening™
System Access Audit Appliance

System Access Audit Appliance


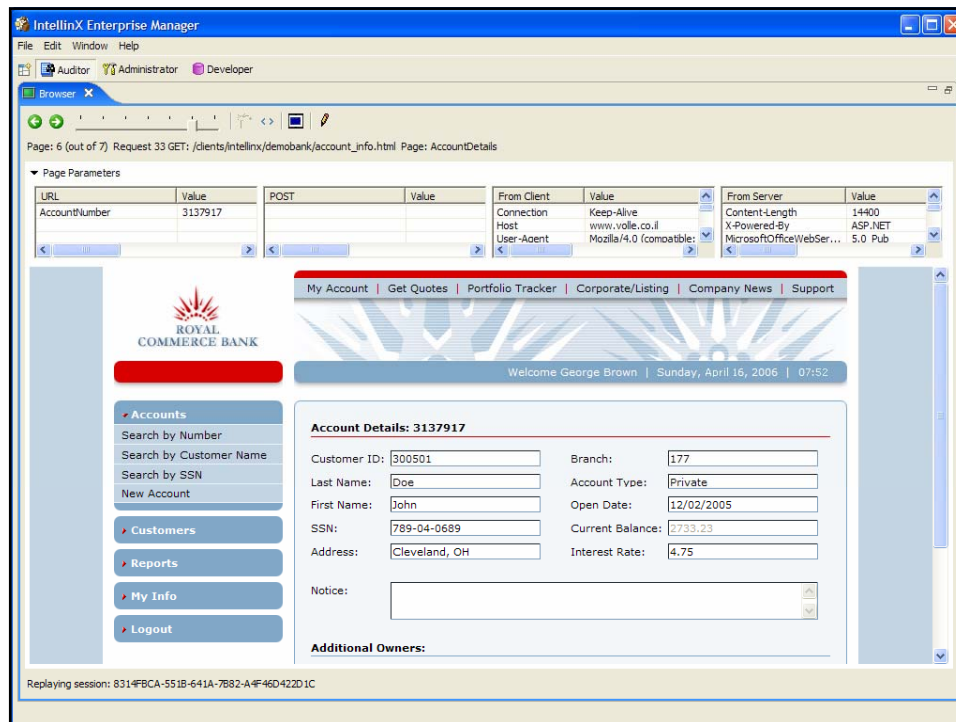
User Activity Replay Demo



Illustruro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC


SDForum-34



Real Case Demo

Leaking Information of Celebrities (VIP)

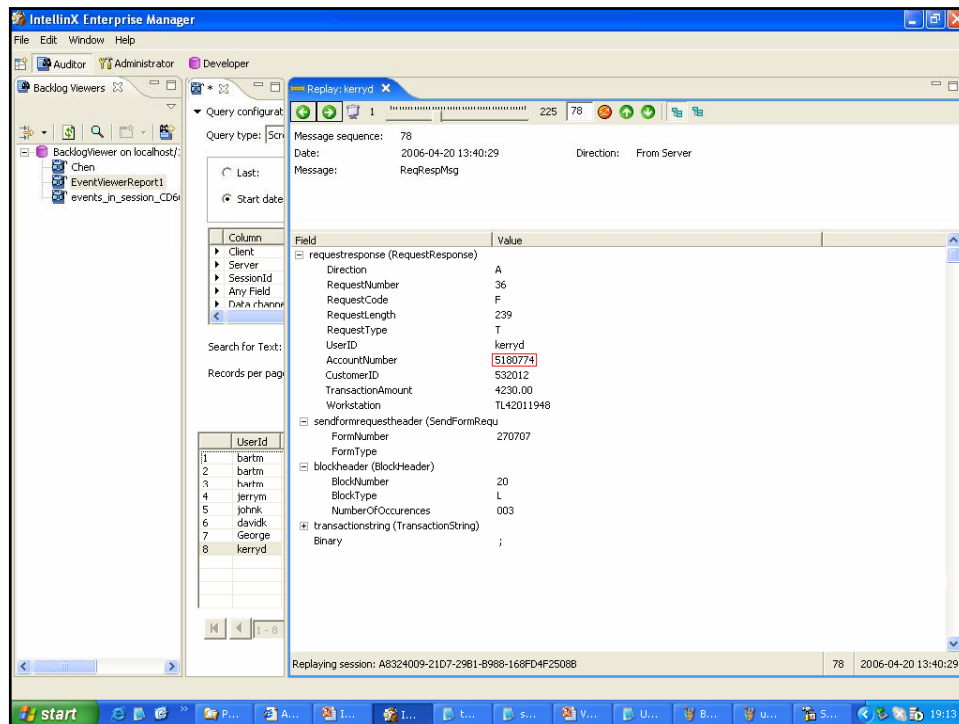
There has been an indication that sensitive information pertaining to account number **5180774** has been leaked from inside the organization to an external source sometime between April 16th and 23rd of 2006.




illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

SDForum-36







Real Case Demo

IT personnel: risk of sabotage?

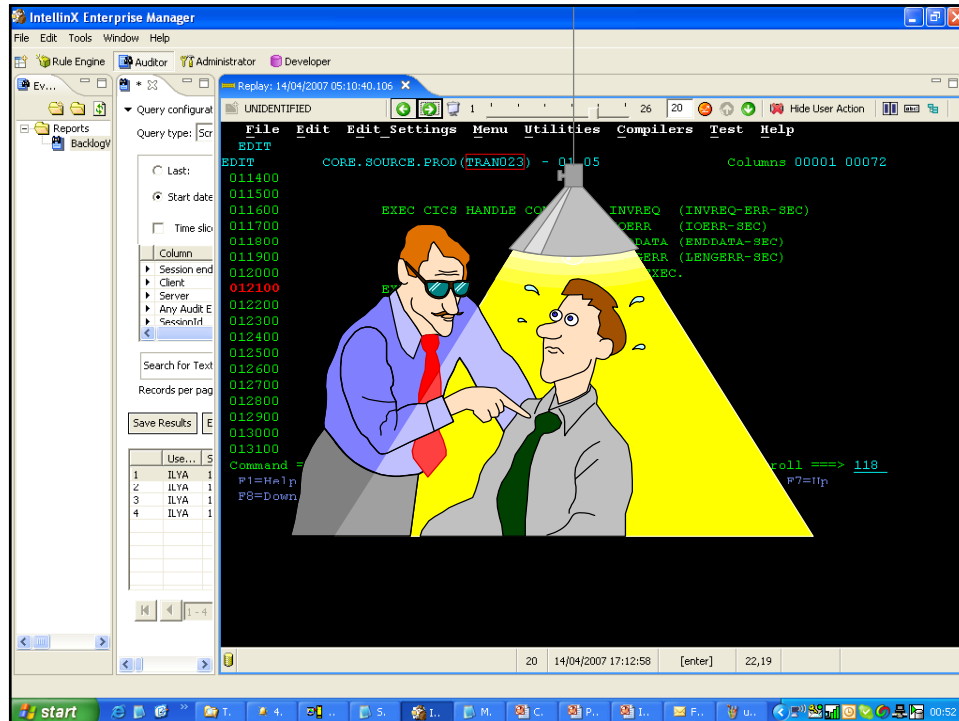
There has been indication that mainframe program TRAN023 has been performing strange database activity which cannot be explained.






Copyright © 2008 illustro Systems International, LLC

SDForum-38






System Access Audit Appliance

*Know What's Happening™
System Access Audit Appliances*

Detecting internal fraud

- Granular Audit Trail allows detailed investigation
Example: Search for all the users who accessed a specific account number
- Adding Controls to sensitive processes
Example: Alert on updating credit limit that exceeds \$100,000
- Identify user Behavior patterns
Examples:
 - Excessive usage of specific transactions
 - Odd hours usage of specific processes
 - Excessive access to high profile accounts
- Tracking privileged users actions
Example: Update of sensitive data in the production environment by the DBA



Copyright © 2008 illustro Systems International, LLC

SDForum-40



System Access Audit Appliance

Regulatory Compliance

Privacy Regulations – GLBA, HIPAA, CA SB 1386

- Detailed logging: Who? Did What? To which data? When? Where from? How?
- Read access included in the audit trail


Sarbanes-Oxley

- Add effective controls to sensitive processes that affect the financial reports
- Add Compensating controls for:
 - ✓ Tracking privileged users activity
 - ✓ Ensuring segregation of duties
 - ✓ Monitoring Change Management




Copyright © 2008 illustro Systems International, LLC

SDForum-41



Detecting Internal Fraud in Banks

- **Account Takeover**
 - Changes to account statement mailing frequency, search for dormant accounts, change of dormant account attributes
- **Customer Management**
 - User changing a customer address and changing it back within a short period of time
- **Unauthorized Customer Limits Bypass**
 - Consecutive credit limit change for same account, Change of credit limit and change back after a short period of time
- **Money Transfer Redirection**
 - Money transfer without a reference information that explains the purpose of this transfer, Money transfer target account overwritten by unauthorized
- **Shell Accounts**
 - Same address of two unrelated entities, Significantly high amount transfer for this type of account



Copyright © 2008 illustro Systems International, LLC

SDForum-42

Detecting Internal Fraud in Insurance

■ Customer Management

- Changes of address, beneficiary, bank account details

■ Policies Management

- Policy parameter changed by member of a team not handling the customer, Changes to dormant policies or employees' policies, unreasonable low tariff, twisting, Manual update of policy's tariff

■ Claims Processing

- Unauthorized approval of checks, manual update of checks, changing bank account beneficiary, retroactive addition of covered person to collective policy

■ Agents

- Unauthorized changes to advance payment terms, Agent bonus terms changed by unauthorized, targets.



Copyright © 2008 illustro Systems International, LLC

SDForum-43

Detecting Information Leakage

- **Detection based on excessive customer information queries**
especially in the case of call-centers, where customer calls are random
- **Detection based on the way a user is searching for a customer**
for example: use of name based search instead of customer number based search
- **Detection based on relevancy of query type to the employee's job**

Privacy of VIP Accounts (celebrities)

Users that are querying many VIP customer accounts

Users that are querying same VIP customer account multiple times


Searching for a VIP information by name
(not by account number)



Copyright © 2008 illustro Systems International, LLC

A "Healthy Paranoia"

- Abundant network activity has brought u
- Rethink the business
- Look for information "age"
- React when but be sure to notify all appropriate
- Review, Respond, Repeat



illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

SDForum-45

A "Healthy Paranoia"



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

illustro
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2008 illustro Systems International, LLC

SDForum-46