


**DLP to Forensics:
The Face of IT Security and Governance
is Changing**




Presented by
Jeremy Wunsch
Founder and Director of Data Forensics
LuciData, Inc.
Headquarters: Minneapolis
Offices: Denver, New York, Des Moines

Copyright © LuciData 2010

Consider This...

750 Employees' Names, DOB, SS#'s, Salaries, Home Addresses
12 Corporate Credit Card Numbers
A common Stock Option Proposal Memo from the CEO to the Board
of Directors

What do they all have in common?




Copyright © LuciData 2010

FTC: Data breaches linked to P2P services

February 23, 2010

The FTC sent letters to 100 organizations where personal data, including Social Security numbers, had been leaked through peer-to-peer web services. The organization said it had discovered the widespread data breaches at companies, schools and local governments.

"Unfortunately, companies and institutions of all sizes are vulnerable to serious P2P-related breaches, placing consumers' sensitive information at risk," FTC Chairman Jon Leibowitz said in a news release.



Copyright © LuciData 2010


P2P File Sharing breach

A Pfizer Inc. employee who installed unauthorized file-sharing software on a company laptop, has exposed the Social Security numbers and other personal data belonging to about 17,000 current and former employees at the drug maker.

Of that group, about 15,700 individuals actually had their data accessed and copied by an **unknown number** of persons on a peer-to-peer network

Such incidents highlight the importance of implementing controls for preventing either accidental or deliberate data leaks

Source: Computerworld




Terminology: Risk vs. Threat

Internal Threat
The potential for a person, program, or process to take advantage of a vulnerability, from within the organization and cause financial loss.

- Threat arises from intention; risk does not.
- Threat requires identification; risk does not.

Accidents happen.

So does exploitation.




Vulnerability and Loss

Which companies are vulnerable?
From the small partnership to the international conglomerate, all companies are vulnerable. No one is immune.

What does a company stand to lose?

- Intellectual Property
- Employee Trust
- Competitive Advantage
- Sensitive Data
- Customers
- Market Cap
- Productivity



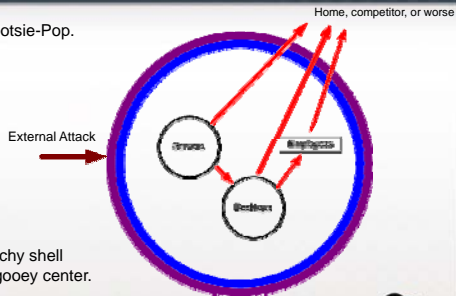
Where are the Vulnerabilities?

- Corporate Email
- External Email (Yahoo!, Hotmail, Comcast...)
- Instant Messaging
- Chat Rooms
- Bulletin / Message Boards
- Peer-to-Peer (P2P)
- Blogs
- USB Drives (and the like)
- iPods
- Lost or stolen equipment and data
- Social Media (Web 2.0)
- Smart Phone (Blackberry, iPhone)



Information Security Today

It's like a Tootsie-Pop.



A hard crunchy shell with a soft gooey center.

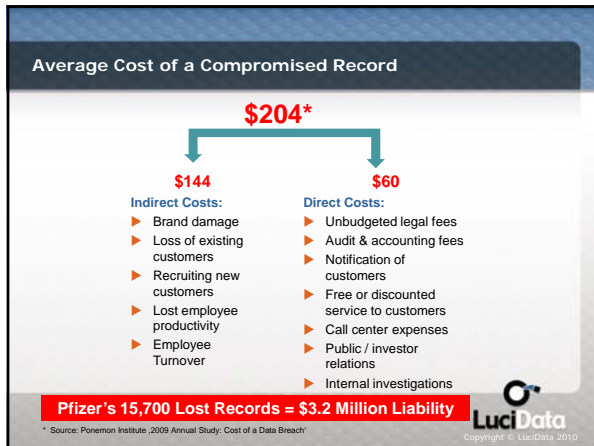


"The Survey Says..."

- **45 % of professionals have taken corporate data with them when they changed jobs**
 - Many of them simply e-mailing it to themselves or storing it on a peripheral device
- **42 % said that corporate security measures were inadequate**
- **53 % on average were also of the opinion that their employer's intellectual property was being used by a competitor**
 - The number of IT professionals who felt that way rose to 63 %

Source: IT Compliance Institute







Governance Defined

Established roles, responsibilities, policies and processes providing direction, guidance and control over the use of organizational technologies in driving to meet business goals.

Effective governance anticipates the goals and needs of both IT and business units, providing guidelines that include deployment, compliance, security, best practices and return on investment.




Internal Threats




Bulletin Board Betty

Regularly posts to public message boards and enjoys sharing breaking news with others.




Departing Dan

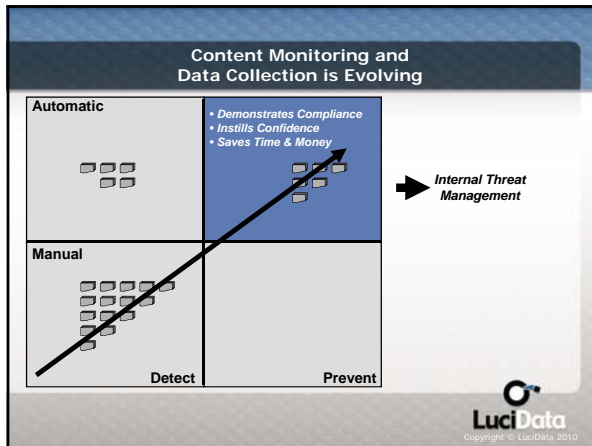
Hands in 2 weeks notice and removes valuable information via USB Flash Drive



Call Center Clyde

A Call center employee has access to sensitive customer information and electronically sends the information outside the corporate network.





- ### Internal Threat Management
- Internal Risk Assessment
 - Data Classification
 - Policy, Standards and Procedures
 - DLP - Content Monitoring**
Email, Webmail, IM, Chat, P2P...
 - DLP - Device Control**
 - Disk Encryption**
Use Full Disk Encryption Software that works with Forensics
 - Internal Incident Response Plan
 - Data Forensics**
 - Litigation Readiness
- Copyright © LuciData 2010

What is DLP

Data Loss Prevention definition at Wikipedia:

systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), and with a centralized management framework. The systems are designed to detect and prevent the unauthorized use and transmission of confidential information.

also referred to as; Data Leak Prevention, Information Leak Detection and Prevention (ILD), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) or Extrusion Prevention System

DLP is Proactive

Copyright © LuciData 2010

DLP and Data Forensics in Court

- There is NO silver bullet in Court when dealing with the DLP
 - You can put solutions together to get multiple bullets to win
- No known court case that solely used a DLP to win
- DLP is used as a “spotlight” to find a problem/issue
- Forensics is used to verify the problem/issue for Court
- Following proper data forensic procedures is needed for electronic evidence to hold up in Court



Is Full Disk Encryption DLP?

There is a lot of question if encryption should be considered DLP

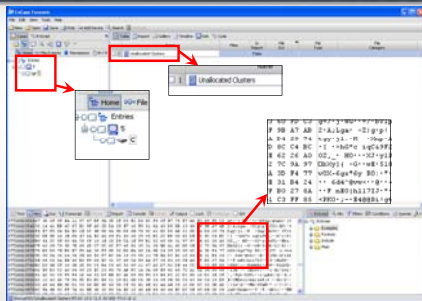
Based off the definition given earlier does disk encryption

- Protect data at rest
- Centralized management framework.
- Prevent the unauthorized use and transmission of confidential information.

Therefore Full Disk Encryption can be considered a portion of a full DLP solution



Forensic View of Encrypted Drive



Before Installing DLP Solutions

- Do you have policies and procedures in place that allow monitoring of ALL network traffic?
- What do you want to monitor?
 - What rule sets do you want to have turned on?
- Do you have a proxy?
 - Encrypted content (HTTPS)?
- How many egress points do you have?
 - Where do you need to place the network device to be able to capture what you want to monitor?
- What enforcement capabilities are there?
 - Who will monitor the solution?
 - What type of escalation is needed for specific events?
- Is the solution going to effect other technology or business units?



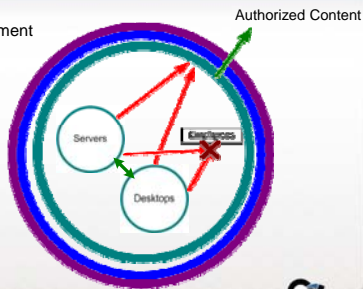
Unintended Consequences of DLP

- Increased communication between IT, Legal, Compliance, HR and other business units
- There will be greater need for data forensic capabilities
- There will be more litigation but it will be easier to win
 - Most things will never make it to court due to the abundance of evidence
- Initial staff turnover
 - Reducing non-productive staff
- Identification of training needs
- Verification that IT security measures are working correctly.
- Change in business units processes and procedures



Monitored Data Protection Ring

- Internal Threat Management
- Content Monitoring
- Device Control
- Encryption
 - Whole Disk
 - Partial Disk
 - Content



Questions?



Jeremy Wunsch
Founder and Director of
Data Forensics
(o) 612.326.3456
jwunsch@lucidatainc.com

www.lucidatainc.com