



# Opening Pandora's Box:

## The Case for Data Auditing

*"Data audit should be an integral part of operations. Not only does it augment rigorous perimeter security by actively logging all access to all data, data audit provides invaluable protection inside an organization - where an organization is most vulnerable"*

Baroudi Bloor Research Analysts, 2004

---

## **Executive Summary**

This paper identifies a series of push and pull factors that justify data auditing. 3 key areas are addressed: return on investment, the need to defend yourself against the insider threat, and FSA/legislative compliance.

Jario's R.O.I is genuine and provable at every knowledge workers desktop. The established formula:

$$\text{Cost of Information} = \text{Document Preparation Cost} / \text{Rate of Reuse}$$

requires you to decrease duplication of effort if you wish to increase productivity. Data Auditing delivers by establishing what the ratio is, then identifies where opportunities for improvement exist.

The paper also highlights why Pandora's Box is in fact, already open to those who can and are doing you harm. Data Auditing redresses the balance and gives you the answers first, allowing you to stop others stealing, leaking, losing and abusing your data.

Finally, legislation compels a shift in how compliance is attained. The new wave of post-Enron legislation has created a process/quality control model of compliance. This means ongoing monitoring and improvement is central to compliance success.

Improve productivity, reduce loss, enforce compliance.

---

CONTENTS

INTRODUCTION ..... 1  
**Introduction** ..... **1**

THE ROI OF DATA AUDIT ..... 2  
**Productivity** ..... **2**  
**Disclosure cost savings** ..... **2**  
**Reduction in Legal Fines** ..... **3**

THE FACTS ABOUT INSIDER THEFT AND ERROR..... 4

THE LEGAL ARGUMENT..... 5

PANDORA’S BOX IS ALREADY OPEN..... 6

COMPLIANCE AND FSA REGULATIONS ..... 7  
**Controls** ..... **7**  
**Records Management** ..... **7**  
**Disclosure requirements** ..... **7**  
**Chinese Walls** ..... **8**  
**Auditing and Monitoring** ..... **8**  
**Responsibility** ..... **8**

SUMMARY ..... 10

HOW TO PLAN FOR A DATA AUDITING EXERCISE ..... 11

WHAT CAN YOU EXPECT TO LEARN FROM A DATA AUDIT?. 12

## INTRODUCTION

### Introduction

Jario's Document RADAR product is used to track and monitor every file created, accessed or moved across the entire network, from laptop to disk drive to network share devices and NAS.

"Jario knows the who, where and what happened to every file."

A number of key benefits come from auditing the use of your firms and your client's intellectual property. The key objection raised by potential customers is the fear that by installing the RADAR, they will in effect open a Pandora's Box of compliance and process failures they do not wish to be aware of. In effect "What I don't know can't hurt me or my firm."

This paper will address this concern by demonstrating the value in knowing what is happening to your IP. The paper also addresses the costs you are currently incurring by ignoring the misuse of corporate data on the desktop.

Why should you open Pandora's Box? We will focus on the following topics:

1. The ROI of Data Auditing
2. The facts about insider theft and misuse of corporate data.
3. The legal argument
4. The increasing risk from E-Discovery
5. FSA Compliance

|                     | Worked On | Viewed | Printed | Emailed Externally | Web Based Email | Emailed Internally | Not Backed Up |
|---------------------|-----------|--------|---------|--------------------|-----------------|--------------------|---------------|
| Total               | 380       | 690    | 0       | 107                | 4               | 140                | 928           |
| Average             | 27        | 49     | 0       | 7                  | 0               | 10                 | 66            |
| Max                 | 82        | 216    | 0       | 69                 | 2               | 69                 | 294           |
| Min                 | 0         | 0      | 0       | 0                  | 0               | 0                  | 0             |
| Username            | Worked On | Viewed | Printed | Emailed Externally | Web Based Email | Emailed Internally | Not Backed Up |
| Administrator       | 2         | 0      | 0       | 0                  | 0               | 2                  | 6             |
| Stephen Murtagh     | 49        | 79     | 0       | 0                  | 0               | 4                  | 80            |
| Graham Cruickshanks | 23        | 41     | 0       | 2                  | 0               | 11                 | 70            |
| Andrew Smith        | 0         | 0      | 0       | 0                  | 0               | 0                  | 1             |
| Stephen murtagh     | 0         | 1      | 0       | 0                  | 0               | 0                  | 0             |
| Chris Oliver        | 77        | 176    | 0       | 2                  | 2               | 8                  | 93            |

*An example of a summary report from a Jario RADAR installation.*

---

## THE ROI OF DATA AUDIT

Three areas are addressed:

- Productivity
- Legal Costs
- Risk Reduction

### Productivity

Knowledge workers are not monitored in terms of statistical work done. They cannot be rewarded by volume as more words and documents can mean lower, as well as higher productivity.

Kingsley Martin, a lawyer with a special interest in knowledge management, has provided us with a simple and accurate formula about the Return on Investment in Knowledge.

$$\text{Cost of Information} = \text{Document Preparation Cost} / \text{Rate of Reuse}^1$$

i.e. The more a document is used, the greater the return against the cost of creation.

Kingsley's difficulty just 18 months ago however, was, as he had no access to a Jario like Data Auditing tool, how did he:

- a. Know what his firms' current ratio was?
- b. Identify how to improve it?

Data auditing is the answer. By reporting and tracking file use to both end users as well as managers, users can be guided to the data they should be using, rather than doing the same work twice.

PWC identified that the average knowledge worker spends more than 15 minutes a day just trying to find data on their own network. It is unknown how much time is wasted redoing the same work others in a firm have already completed.

Users also waste time and make mistakes by updating older copies of documents, unaware that further changes have been made by others.

### Disclosure cost savings

Steven Whetson a senior litigation partner at internationally renowned Testa, Hurwitz

---

<sup>1</sup> Kingsley Martin, 2002 - <http://www.llrx.com/features/kmroi.htm>

---

and Thiebault was very clear about cost savings. Not only would he prefer to defend a client who had a data audit tool, but that the costs to his client of his defence would be lowered substantially by giving him access to Jario like records.

The costs and pain of discovery always outweigh the costs and risk reduction of knowing the answer first.

Other examples:

- PDI Inc pharmaceuticals recently spent more than \$3million on a relatively simple disclosure exercise, indexing the content they had on their network for analysis. Disclosure is the painful after the fact search. With Jario preinstalled, they could have asked the question of the Jario audit server centrally and received an immediate response without a fee.
- Law firm Dinsmore and Schohl identified they spend more than \$200,000 per annum to simply dedupe the records they hold on their various systems.

### Reduction in Legal Fines

Pfizer pharmaceuticals were fined \$430 million because their sales agents were found to be illegally marketing their drugs. An effective, desktop & network data audit tool would have flagged changes made to marketing materials at the salesman's end of the line immediately.

The image is a screenshot of the CNN International website. At the top left is the CNN International logo. To the right is a blue banner with the text "For solutions to today's security problems". Below the logo is a search bar with "SEARCH" and "The Web" and "CNN.com" options. A navigation menu on the left lists categories like Home Page, World, U.S., World Business (highlighted), Technology, Science & Space, Entertainment, World Sport, Travel, Weather, Special Reports, ON TV, and What's on. The main content area features the headline "WORLD BUSINESS" and "Pfizer fined \$430m in drug case". Below the headline is the date "Friday, May 14, 2004" and the text "WASHINGTON (Reuters) -- Pfizer Inc. has agreed to pay \$430 million and plead guilty to criminal charges for illegally...". To the right of the article is a "YOUR E-MAIL ALERTS" box with a radio button for "Pfizer Incorporated".

Abbey National were recently fined a seven figure sum for failing to provide investigators with the required documents to indicate compliance with money laundering provisions. Those documents should never have been lost. An alert mechanism within the process would have stopped accidental deletion or forced compulsory backup, whichever process was at fault.

---

## THE FACTS ABOUT INSIDER THEFT AND ERROR

By insiders we mean the employees of your firm. Short and simple, here are the facts on Insider Theft:

- 85% of all firms lost data from insider behaviour in 2002. *FBI 2002.*
- 85% of all data theft is committed by insiders. *Ernst and Young 2003.*
- The number of internal data theft incidents reported to the authorities doubled between 2002 and 2003. *Carnegie Mellon Institute 2003.*
- 60% of all electronic financial fraud involves an insider. *PwC 2003.*

There is also another equally financial costly and reputation damaging fact about Insider behaviour with your data:

- 88% of all unwanted deletion of data is caused by human error - i.e. the "Whoops, I shouldn't have deleted that" feeling. *Broadcasters Network International, 2003.*

A single record accidentally deleted has cost the likes of Abbey National and other major financial institutions 7 figure fines due to breaches of money laundering regulations.

On a different scale, 70% of SME firms that experience a major data loss go out of business within 1 year. *Sunday Times 2003*

From an organised attack to an employee sending confidential information to the press or to your competitors, we GUARANTEE you, someone in your firm is either deliberately stealing or accidentally leaking crucial data as you are reading this paper.

You currently don't know who, and even if you did, you would have very little in the way of evidence to prove it.

---

## THE LEGAL ARGUMENT

At the core of the "What I don't know can't hurt me" argument, is the fear that your firm will become legally exposed as you may discover evidence of wrongdoing.

The case against this belief is made simply:

***"I would rather defend a firm who has Jario than without."***

Stephen Whetson, 2004

This quote was given directly by Stephen Whetson, senior litigation partner at US technology law firm Testa, Hurwitz and Thiebault. His more detailed explanation follows:

"The tool's ability to provide various data about the circumstances surrounding the creation, transmission, receipt, and duplication of a file could be of great value in the litigation context. In criminal and civil litigation, government investigations, and internal inquiries, lawyers and clients often need to search for this kind of forensic data concerning a particular document or set of documents (e.g., when was a side letter created, who created it, who was it sent to and when, do other copies exist under different names?, etc.). The tool should make that job much easier and, thereby, save clients substantial costs by avoiding having their lawyers conduct those searches manually or semi-automatically (using other vendor services). "

So not only is the legal view positive about the value of helping a client defend itself from legal recourse, but a lawyer is actually prepared to suggest it would lower the costs of that defence!

This leads us neatly to the next section.

---

PANDORA'S BOX IS  
ALREADY OPEN

Your employees know where the data is and can freely access and disseminate anything they see with absolute ease.

The FSA is entitled under the provisions of its investigatory and "mystery shopping" provisions to access your data and systems. It does so using Electronic Discovery software.

There are currently more than 100 software companies who produce electronic discovery applications. These programs work retroactively in attack mode, the opposite to Jario's defensive, proactive stance. They are utilized by prosecutors, auditors and regulators like the FSA or SEC to find electronically stored information that will form the case against you.

(See [www.eedinc.com](http://www.eedinc.com) as an example.)

Electronic Discovery, originally the preserve of US litigation, is now central to UK investigation of financial irregularity. The FSA use these tools to their full, the recent mutual fund investigation and subsequent fines are a prime example of how evidence was easily found. Major law firms including the magic circle and specialist IT litigation departments in firms like DLA and Masons use e-discovery on an increasingly regular basis. They can identify evidence both to defend their clients against those prosecuting with e-discovery tools and to do the prosecuting.

In short, you are blind, your competitors, regulators, auditors and potential prosecutors are not.

---

## COMPLIANCE AND FSA REGULATIONS

The following is intended as a set of references to illustrate the sheer volume of very specific FSA regulations now in place.

A company must be able to:

Capture, Store and Retrieve any Record within 48 hours, there are 6 key themes within the FSA regulations that Jario applies too:

1. Systems and Controls
2. Records Management
3. Disclosure
4. Chinese Walls
5. Auditing/Monitoring
6. Responsibility

### Controls

You must have appropriate systems and controls in place to track all electronic documents and communications:

- SYSC: 3.2.6: Compliance
- SYSC: 3.2.11: Management Information
- APER: 4.6.8: Failing to Supervise
- APER: 4.7.3: Failure to Implement

### Records Management

It is fundamental to be able to capture, store, and retrieve any file on demand.

- PRIN: 3.2.20: Records
- COB: 3.7.1: Requirement to make and retain
- COB: 3.7.2: Content of Records
- COB: 3.7.3: Retention
- Money Laundering: 7.3.2: Records Retention

### Disclosure requirements

You must be able to prove your compliance by disclosing data to regulators, auditors

---

and your own management on demand.

- SYSC: 3.2.11: Management Information
- SYSC: 4.2.2: Internal Procedures
- APER: Principle 4
- APER: 4.4.4: Failure to report promptly
- COB: 1.4.3: Market Conduct
- Supervision: 2.3.3: Access to Documents
- Supervision: 2.4.3: Mystery Shopping
- Auditors: 3.8.3: Supply of Documents
- Auditors: 3.8.6: Conflict of Interest Proof
- Auditors: 3.8.10: Statutory Duty to Report
- Enforcement: 2.3.2: Requiring Documents

### Chinese Walls

In various industry specific scenarios, you must be able to prove you have separated data from different internal departments such as the Tax advice and auditing departments inside a consulting firm.

- COB: 2.4.4: Chinese Walls
- Supervision: 3.8.6: Conflict of Interest

### Auditing and Monitoring

Management must respond to failure by monitoring for repeat behaviour.

- SYSC: 3.2.11: Management Information
- APER: 4.7.4: Failure to monitor
- APER: 4.7.7: Failure to Review and Improve
- Money Laundering: 7.2.2: Audit and Assessment of Control

### Responsibility

It is inherent within the FSA regulations that anyone registered with the FSA as an advisor and crucially anyone responsible for a key function such as IT or Compliance is personally liable.

This of course is just the FSA, there are many other pieces of legislation:

- Sarbanes-Oxley
- Basel II

- 
- Data Protection Act
  - Freedom of Information Act
  - Money Laundering Regulations

You will note the 6 themes highlighted in the FSA breakdown, are repeated in most of these other acts.

---

## SUMMARY

This paper has identified a series of push and pull factors that justify data auditing:

1. The ROI is genuine and provable at every knowledge workers desktop.
2. The Box is already open to those who can and do harm you. Data Auditing redresses the balance and gives you control first.
3. The new wave of post-Enron legislation has created a process/quality control model of compliance. This means ongoing monitoring and improvement is central to compliance success.

---

## HOW TO PLAN FOR A DATA AUDITING EXERCISE

In this very new field, the following Guidelines for data audit by Baroudi Bloor Research provide an excellent beginning.

1. Staff and Systems in control of the audit must be independent of the staff and systems you are auditing.
2. The data audit program must be highly flexible so it can audit as much as possible now and accept new data flows in the future.
3. The program must be flexible as compliance rules will change.
4. A single point of control is key.
5. Security within the application is key.
6. The program must be able to clearly identify what the data is, where it is, where it is going, and who is accessing it.
7. Make it complete - a system that audits half the data, is not worth 50% of the price of a system that monitors all the data.
8. Establish normal usage patterns so reporting can focus on changes and anomalies.

**Jario delivers on these system design goals.**

## WHAT CAN YOU EXPECT TO LEARN FROM A DATA AUDIT?

Below is a sample list of the types of questions a data audit can answer:

- Who is sending what data outside the firm?
- Who is sending data to webmail accounts?
- Who is burning data to cd-roms and usb sticks?
- Who is sending data into the firm and who is receiving it?
- What proportion of my data is exposed to theft or loss?
- What proportion of my records are protected in a records management environment?
- Who are my most and least productive knowledge workers?
- Which documents are the most read in the company?
- What are the new trends on document use this day/week/month?
- Who has seen any specific file?
- Who has worked on which out of date template files?
- What is the document traffic to and from a competitor's domain?

Jario knows the who, where and what happened to every file.

The screenshot displays the Jario Chronicle Viewer interface. The main window title is "Jario Chronicle Viewer - C:\Documents and Settings\Chris Brighthouse\Desktop\Jario\_Executive\_Summary\_Presentation\_v12.ppt". The interface includes a menu bar (File, Tools, Help) and a toolbar with a "Refresh" button. The main content area is divided into two sections: "Version History" and "Locations".

**Version History Table:**

|                                       | created               | modifier                 | safe       | branches | locations | sent     | received | baseline                                |
|---------------------------------------|-----------------------|--------------------------|------------|----------|-----------|----------|----------|-----------------------------------------|
| <input type="button" value="SELECT"/> | 27/05/04 09:33        | Peter Mann               | yes        | 0        | 1         | 0        | 0        |                                         |
| <input type="button" value="SELECT"/> | <b>25/05/04 14:25</b> | <b>Chris Brighthouse</b> | <b>yes</b> | <b>1</b> | <b>3</b>  | <b>1</b> | <b>0</b> |                                         |
| <input type="button" value="SELECT"/> | 09/04/04 09:45        | Chris Brighthouse        | no         | 0        | 2         | 2        | 0        | <input type="button" value="BASELINE"/> |
| <input type="button" value="SELECT"/> | 31/03/04 17:15        | Chris Brighthouse        | no         | 0        | 4         | 2        | 2        | <input type="button" value="BASELINE"/> |
| <input type="button" value="SELECT"/> | 31/03/04 16:49        | Chris Brighthouse        | no         | 0        | 1         | 1        | 0        | <input type="button" value="BASELINE"/> |

Show Deleted Versions

**Locations Table:**

| name                                         | safe  | computer      | domain |
|----------------------------------------------|-------|---------------|--------|
| Jario_Executive_Summary_Presentation_v12.ppt | email | JARIO-LAPTOP1 | JARIO  |
| Jario_Executive_Summary_Presentation_v12.ppt | temp  | JARIO-LAPTOP1 | JARIO  |
| Jario_Executive_Summary_Presentation_v12.ppt | yes   | JARIO-SERVER0 | JARIO  |

Show Deleted  Show Temporary  Show Email

Server: jario-server0 Port: 8083 Server Status: Connected

*An example document report from Jario, showing all activity relating to a set of document versions.*

---

Jario Ltd  
International House  
Hamilton International Park  
Glasgow  
G72 0BN

For more information on this subject please go to [www.jario.com](http://www.jario.com)

© Jario Ltd 2004