



WHITE PAPER

# Protecting the Printed Paper from Data Loss

---

Release No: 1.0  
Date: 10/03/2008

RadianTrust is a brand through which RadianTrust Pte Ltd offers security solutions, services and consultancy in Singapore.

## Table of Contents

1	Introduction .....	3
1.1	Data Loss on Paper:.....	3
1.2	Impact of data loss or leakage: .....	4
2	Approaching Data Loss .....	6
2.1	Step 1: Identify Sensitive Data .....	6
2.2	Step 2: Create Access Matrix.....	7
2.3	Step 3: Protect the Gateway .....	7
2.3.1	Authorised Printing .....	8
2.3.2	Integrity or Anti-forgery.....	8
2.3.3	Counterfeiting or Duplication .....	8
2.4	Step 4: Trace and Patch .....	8
3	Deploying a Security Controls to Protect and Trace Your GateWay.....	10
3.1	Step 1: Identify Sensitive Data .....	10
3.2	Step 2: Create Access Matrix.....	10
3.3	Step 3: Protect the Gateway .....	10
3.3.1	Authorised .....	10
3.3.2	Integrity or Anti forgery .....	11
3.3.3	Counterfeiting or Duplication .....	11
3.4	Step 4: Trace and Patch .....	13
4	Conclusion .....	14

## 1 INTRODUCTION

Data is one of the important aspects in all our business operations today. Just like the match that lights a candle, a company is operational only when there is data. As such data is one of the important assets that are critical to the running of all businesses, yet more than 215 million electronic records have been breached since January 2005, according to Privacy Rights Clearinghouse<sup>1</sup>, a non-profit consumer information and advocacy organization.

### 1.1 Data Loss on Paper:

Data Leakage does not only occur in the digital domain of electronic documentation or transaction. Data Leakage or Data Loss occurs in the printed document by authorised staff is a genuine concern that cannot be swept under the carpet. Statistics have shown that many leakages are due to unintentional action from internal staff, for instance staff printing work to be brought home.. Though this could be done with totally no malicious intent, we could not ignore that there are some cases of malicious intent due to disgruntled employees.

Data loss protection on paper is an issue that companies need to address with. This is especially so as many papers are printed daily for ease of discussion or reading purposes. An article written by World Resources Program states that

*"Computers and information technology have led to more paper consumption, not less."*<sup>2</sup>

In another paper *The Myth of the Paperless Office*<sup>3</sup>, Abigail Sellen and Richard Harper use the study of paper as a way to understand the work that people do and the reasons they do it the way they do. The authors argue that paper will continue to play an important role in office life. Rather than pursue the ideal of the paperless office, we should work toward a future in which paper and electronic document tools work in concert and organizational processes make optimal use of both.

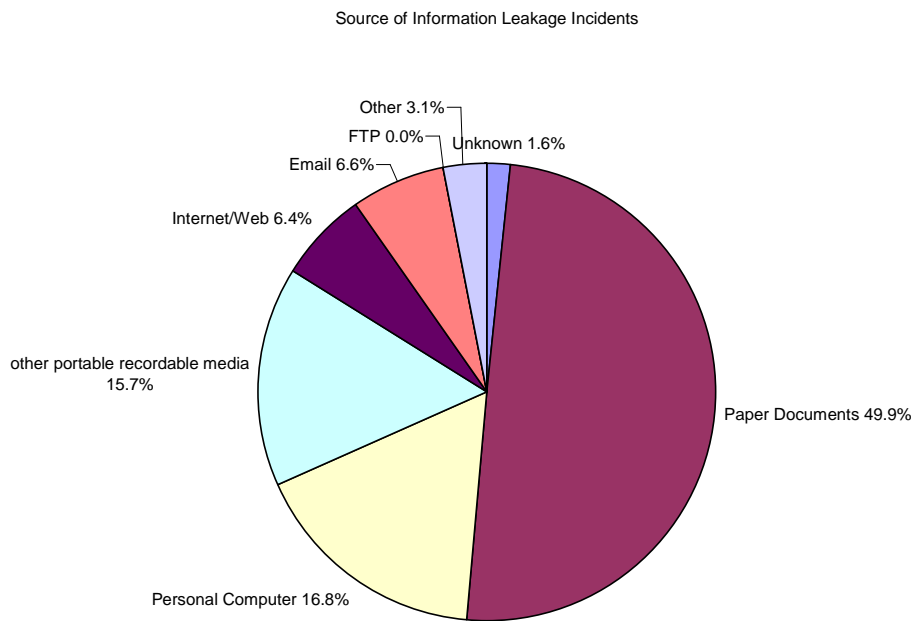
---

<sup>1</sup> Privacy Rights Clearinghouse ([www.privacyrights.org](http://www.privacyrights.org))

<sup>2</sup> Title of article: NO END TO PAPERWORK

([http://earthtrends.wri.org/features/view\\_feature.php?theme=6&fid=19](http://earthtrends.wri.org/features/view_feature.php?theme=6&fid=19))

<sup>3</sup> *The Myth of the Paperless Office* (ISBN-10: 0-262-19464-3 ISBN-13: 978-0-262-19464-8) by Abigail Sellen and Richard Harper



**Figure 1 Source of Information Leakage Incidents<sup>4</sup>**

Studies have been conducted both in the usage of paper in office and the impact of data loss. A Japan Network Security Survey on Information Security Incident Report, review that the percentage of leakage through paper documents occupies almost 50% of the total Information leakage incident. From here we have seen that the risk of data leakage and losing valuable data in the paper form is as real as sending data to unauthorised recipient via email whether it's unintentionally or intentionally.

## 1.2 Impact of data loss or leakage:

The impact of a data loss or leakage brings with it the risks of

- Losing company's Intellectual Property.
- Business information that could results in loss of competitive edge
- Sensitive data such as personnel's information or customers' information

Besides the United States, many countries are looking into passing legislation on the disclosure of any Data Loss or Leakage to the public.

In the United States, Laws and regulations such as HIPAA (Health Insurance Portability and Accountability Act), Gramm-Leach-Bliley and numerous state laws are requiring

<sup>4</sup> Source: NPO Japan Network Security Association:2005 Information Security Incident Survey Report ver1.0

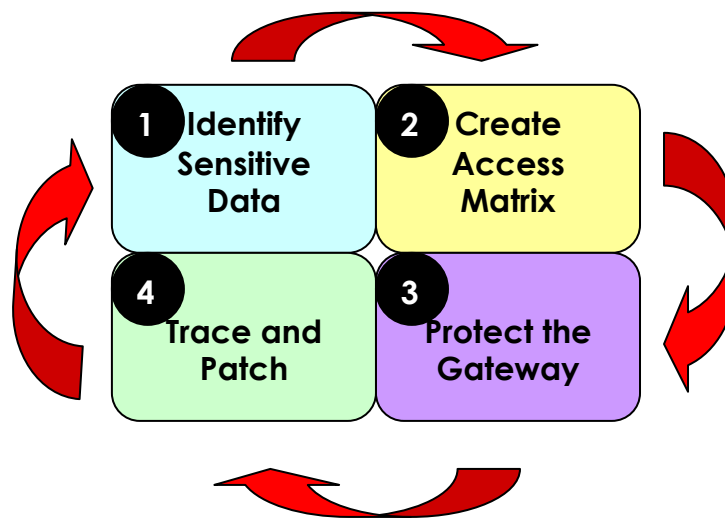
that customers be notified when their personal information is stolen or lost. This implies that any data loss and leakage suffered by the company brings with it:

- The potential loss of business reputation
- The potential loss of credibility of a business to handle its information
- The potential loss of confidence in its customers.
- Possibility of law suits and compensation as such under the Data Protection Act 1998 (U.S.)

## 2 APPROACHING DATA LOSS

However business could take proactive steps in approaching data loss on paper. This includes adopting best practices and implementation of technologies.

An overview of a Data Loss protection for printed paper is as follows:



**Figure 2 RadianTrust Methodology to approaching Data Loss on Printed Paper**

### 2.1 Step 1: Identify Sensitive Data

Data carries different values in retrospect to the nature of the businesses, what is sensitive to one, does not necessary be sensitive to another. For instance, the employee names of a consultancy agency do not carry the sensitiveness of the employee names of secret spy agencies. The former distributes the names of its consultants to its customers publicly, while the other remains secret in order for a job to be done.

Therefore what data is most sensitive to your business? The tasks at hand are to:

- Identify the different departments and lines of business.

- Identity both the regulatory and non-regulatory security needs e.g. the Finance department and the Data Center would have different controls and standards to follow. An application hosted for a customer would carry a different security classification, for instance a office pay system would carry a confidential classification compared to an employee's leave management system.
- Identity what are the applications from which the data are generated from before printing.

## 2.2 Step 2: Create Access Matrix

After knowing where the different requirement and needs for data to be printed, the next steps is to identify the authorised person to print these data.

- Identify who have access to this information.
- Identify who should be the authorised people.
- Identify if there is a legitimate need for printing by these people and the required copies.

Knowing where the sensitive data and who should have this data provide the inputs to create an Access Matrix for the implementation of policies. Access Matrix is created by mapping the authorised person for each of the application where sensitive data are printed from.

An example of a Matrix is as follows:

Staff	Application	Data	No. of copies
Finance Administrator	Finance System	Accounts payable	2 (Master and Duplicate)
HR payroll executive	HR Employee System	Staff pay slips	1 pay slips per staff name

**Figure 3 Example of an Access Matrix**

## 2.3 Step 3: Protect the Gateway

Having the Access Matrix on hand, polices could be implemented to control and safe guard the printed copies of data by authorised people.

Protection of the data as it's printed from the digital form to the paper form is an important aspect. The security considerations are further broken down to the following:

- Authorised
- Integrity or Anti forgery

- Counterfeiting or Duplication

### 2.3.1 Authorised Printing

When people are restricted to the number of copies they could print, careful consideration and extra caution would be given to the handling of the print-out. For instance, if only 2 copies can be printed, a staff would not be likely to print copies for reading purpose unless it's absolutely required.

### 2.3.2 Integrity or Anti-forgery

Data could be lost when an authorised original document is altered. Such as a printed invoice is altered before it reaches the finance department. Alterations of data on printed document without means of detection put any businesses in a risk.

### 2.3.3 Counterfeiting or Duplication

Printed Document could be duplicated and circulated as originals. The question that comes to mind is: are we able to protect the original document and allows people to tell if the data on a document has been duplicated? One of the common issues people faced when presented with two identical piece of information from knowing which is the original and which is an duplicated copy. An illustration would be a movie eTicket purchased online, when two copies are presented to lay claim on the same seat, how would the cinem's staff be able to tell them apart? Data loss through duplication of the original document and then presenting them back to the company is an issue that could cost greatly for a company.

## 2.4 Step 4: Trace and Patch

Security is a continuous process where policies are reviewed, security controls are implemented and people trained. Therefore it is of utmost importance to be able to trace and patch the situations where printed documents are not handled as they should.

To achieve this, the printed document should include traceability to the person who printed the document. The Traceability information should also be hidden from the staff but allows the security officer to trace the identity of the person printing the original through a security system. This is to protect against people by-passing the system through alterations of this information. The effectiveness of this system also calls for this traceability information to be present in the copied versions of the original document.

Traceability also has another aspect that includes allowing a company to tell if a document is in its original stage or a copied form. If a printed document has been

detected as a copied document and the company security policies restricted distribution of the document, the company would be able to be alerted to a potential breach of the policies and using tracing of the ID, the policies and be further reviewed and more security controls can be revisited.

Knowing that all documents can be traced to the original person who prints the document would also serve as a deterrent to careless handling of printed documents.

### 3 DEPLOYING A SECURITY CONTROLS TO PROTECT AND TRACE YOUR GATEWAY

With the approach to Data Loss for printed document, how do you get started? RadianTrust, with its years in security and implementation of security solutions and services has developed a flagship product that can be integrated with your existing applications or any other security controls without a need for a major overhaul of your company printing infrastructure.

#### 3.1 Step 1: Identify Sensitive Data

RadianTrust has a team of profession services consultant trained in security that would be able to assist you in the identification of sensitive Data. At the end of this step, you would have identified:

1. the Gateways of which sensitive data are generated and streamed to the staff or end-users computer.
2. the groups of staff that handles and prints sensitive information

#### 3.2 Step 2: Create Access Matrix

Creating an Access Matrix allows you to be able to see who is authorised, where they print from and how many should they be allowed to print. This information is important in setting security policies.

#### 3.3 Step 3: Protect the Gateway

Protect the Gateway. In step 1 we would have identified the gateways and the step 2 gives us the access Matrix on which to implement the security policies. In this Step RadianTrust flagship Phidélity provides solutions to integrate with your existing Gateways and complements any of the data loss protection vendors providing digital data loss protection on system to provide a complete solution that extends to paper.

##### 3.3.1 Authorised

**Print Control** feature in Phidélity controls the number of printed copies allowed. Generally, the secure documents will be streamed from the server through the Print Control Service to the printer for printing. Your application can configure and restrict the number of printed copies for authorised people to print.

### 3.3.2 Integrity or Anti forgery

Phidélity comes with a **SecureCODE** feature that help protects your document Integrity. SecureCODE synergised 2D barcodes and public key infrastructure (PKI) technology to store and secure crucial data from within the document. SecureCODE ensures the authenticity, data integrity and non-repudiation for the document and allows easy detection of any document/information tampering.

This allows your document to be verified for the integrity of the data printed in the document. The SecureCODE using PKI technology allows you to verify that the SecureCODE is signed from you or your trusted source. Should the data be altered on the document, the SecureCODE would allow you to compare with the original value. This would enable detection of the Data loss by alteration of the data in the printed document.

SecureCODE also makes provision for important information stored in it to be further encrypted for confidentiality and digitally signed by the issuer.

SecureCODE can be easily and conveniently verified via several offline/online channels:

- Mobile phone
- Fax
- Email
- Web page
- PocketPC
- Software Client (if offline mode required)

Phidélity's decoding options are flexible and based on industry standards – no proprietary software or hardware is required to decode and verify SecureCODE data

### 3.3.3 Counterfeiting or Duplication

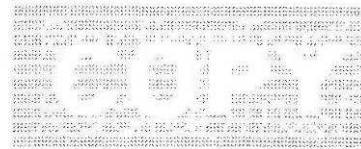
Phidélity **Optical watermark** is an impressive piece of innovation that is embedded in printed document to magically reveal unauthorised attempts to duplicate the document. Verification of document authenticity is made so convenient that it is nothing more than a glance. It is impossible to reproduce protected documents on copiers, cameras and scanners, and pass them off as originals.

The optical watermark in Phidélity consists of two features, a visible watermark and an invisible watermark. The visible watermark can be the company logo or the company name while the invisible watermark can be words like "COPY" or "VOID". Both the visible and invisible watermark will be embedded into the document and printed together with the document via a laser printer.

When photocopied, the visible watermark (i.e. the company logo or company name) will deteriorate, while the invisible watermark will appear. To verify that a document is a photocopied version of the original document, one only has to check that either the visible watermark is not clearly visible or the invisible watermark is clearly seen. No special decoding equipment is required for this verification process of the watermark as the watermark is visible to the naked eye.



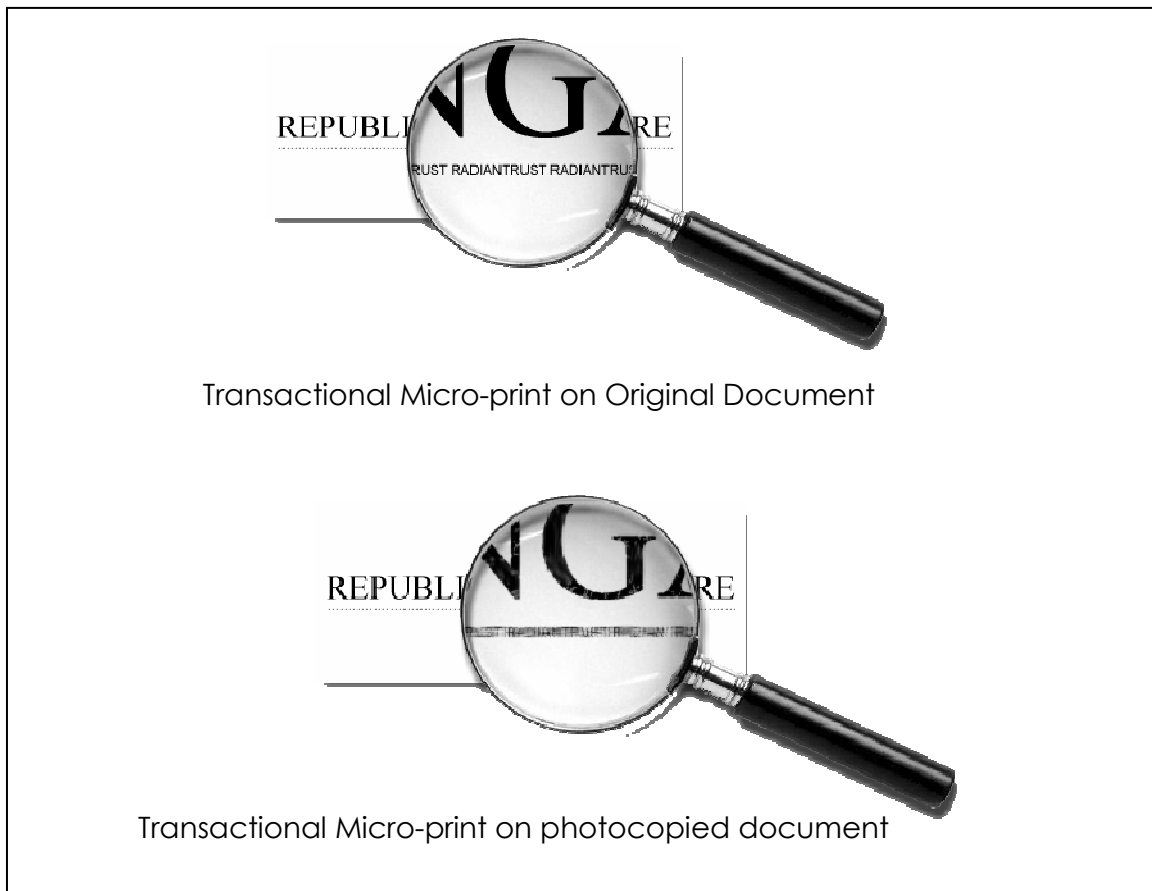
Original



Photocopied

**Figure 4 Optical Watermark Sample**

Besides Optical Watermark, Phidélity's **Transactional Micro-Print** is another layer of security feature for printed document to guard against duplication, an innovative use of very tiny imprints of dynamically generated text, such as the document serial number into the printed documents. Its contents can only be viewed clearly under a magnifying glass. This line of text will be distorted when any attempt is made to duplicate the document optically, thus revealing any unauthorised reproduction of the document. It is simple, yet effective.



**Figure 5 Transactional Micro-print under a magnifying glass**

### **3.4 Step 4: Trace and Patch**

Phidélity's optical watermark also enables tracing of original and replicated document. At the same time, Phidélity understands your needs to trace document and through its continuous Research efforts, has implemented Trace ID to meet this need.

**ID-Trace** feature employs the use of steganography to insert a traceable fingerprint into printed documents. Traceable information, such as the identity of the user who initiated the printing or the date of printing, is covertly embedded into the document. For auditing or verification purposes, this information can later be decoded and verified to assert the identity of the original document holder. This allows corporations to take the necessary corresponding actions to limit further risk and employ other mechanisms to ensure accountability from within.

## 4 CONCLUSION

Many Digital Right Management or Data loss protection solutions target to help companies access their digital data leakage issues. However once the data is printed by authorized personal, the data loss issues on printed paper is usually overlooked and many data are lost and leaked through this channel. Attempt by unauthorized personnel to tamper the printed data is another avenue which data are lost.

RadianTrust, with its years in security has vast experience in integration with numerous applications for governments, trades organizations. RadianTrust's flagship product: Phidélity with its document security features complements your existing Digital Data Loss protection and applications to protect your printed property.