

# Preventing intellectual property abuse

A comparison between information rights management and data loss prevention

Copyright 2009 Danny Lieberman. [danny@software.co.il](mailto:danny@software.co.il) [Software Associates](#)

This work is licensed under the [Creative Commons Attribution License](#).

## Abstract

To paraphrase Lord Kelvin - “You cannot improve what you cannot measure” this paper examines two data security technologies – information rights management (IRM) and data loss prevention (DLP). We lay the groundwork for a comparison by considering the criminal, technical and security aspects of information leakage. In order for a company to decide *what* security countermeasures are best for them – they must *measure* the movement and value of their data, and weigh that in terms of a threat model. We conclude by suggesting a series of questions to ask in order to test two hypotheses – 1) that information leakage is currently happening and 2) that a cost-effective risk mitigation plan can be defined and implemented.

## 1. Introduction

The benefits of patents, in particular in the chemical and pharmaceutical industries, substantially exceed the cost of litigation, providing a strong incentive for new product innovation<sup>1</sup>. However, there are classes of assets not protected by patents: new products in R&D phases, manufacturing process recipes, internal financials and statutory information such as decisions of the supervisory board. Such information is often shared by many people in the company as well as outside contractors and researchers. Typically protected by NDA (non-disclosure agreements), the company can sue a person who leaks information, seeking damages. While the legal costs are sizable, the business costs of litigation for the company can be much higher, moreover, first you have to catch the discloser... Information leaks require managers and researchers to spend their time producing documents, testifying, strategizing with lawyers and appearing in court.

Since the potential financial loss can be significant, companies seek cost-effective security controls that will go beyond an NDA. Two leading candidates are IRM and DLP:

- Information Rights Management (IRM) technologies use cryptography to persistently protect information contained in documents and emails from unauthorized access in and out of the organization. IRM is a digital rights-centric security control which depends on the interaction between a user and the applications that handle the documents. IRM requires the organization to know in advance which information it wants to control
- Data Loss Prevention (DLP) technologies detect and prevent the unauthorized transfer of data. DLP is a data-centric security control, agnostic to rights control and applications. Agent DLP runs on the user PC, whereas network DLP runs in the enterprise network. DLP enables the organization to monitor information flowing in and out of the company, detect and prevent information leaks.

---

<sup>1</sup> “Patent Failure, How judges, bureaucrats and lawyers put innovators at risk”, Bessen and Maurer, Princeton University Press, 2008 pages 130-156, “The cost of dispute”

## 2. The crime of information abuse

Abuse of a company's intellectual property and statutory information involves theft and/or unauthorized disclosure. Like any other crime, in order to steal or disclose assets, a person needs a combination of means, opportunity, and intent.

**Means:** Companies issue users legitimate user accounts with the rights to access certain applications, databases and file services. Insiders have knowledge of how the system works, the business processes, the company culture and how people interact. They know who manages the rights management systems and who grants systems permissions. With the right knowledge and social connections, means can be obtained even if they were not originally granted by design.

An example is the 2008 \$7BN fraud at French bank Societe Generale, committed by a trader who had worked in the bank's audit group. He knew what trades would raise red flags, and what would not, and as a result could fly under the radar. Consider the recent case of an equipment manufacturer. A director of new technologies had thousands of confidential product design and business development documents on his PC. The files were not protected by the company's document control system - simply because they were not part of the manufacturing process yet. In both cases, users had the means and abused their privileges - one with fraudulent trades and the other with deliberate data theft.

**Opportunity:** The second piece in a crime is opportunity. With access to systems and their data, daily interaction with the applications and other users an insider has the opportunity to exploit people and system vulnerabilities and steal data or modify data for personal gain.

**Intent:** The third element is intent. Intent is impossible to control since it depends on human behavior, which may be irrational. In the Societe Generale case, the trader made no personal gain. In other cases, for example, an insider may need to make payments on a house; a bribe can appear to be acceptable when it comes from a person believed to be a friend operating in the person's best interests etc.

Using our [practical threat model](#) of a crime - we can see that IRM mitigates the vulnerability of “**means**“. Once rights are granted by the IRM system – the user is trusted and has rights to access the controlled document. IRM doesn't mitigate threats by trusted users, nor protect assets that are not controlled by the IRM system.

Using the same model, we see that DLP mitigates all three vulnerabilities - “**means**“, “**opportunity**“ and “**intent**“, since it measures movement of data to unauthorized destinations and is independent of rights management.

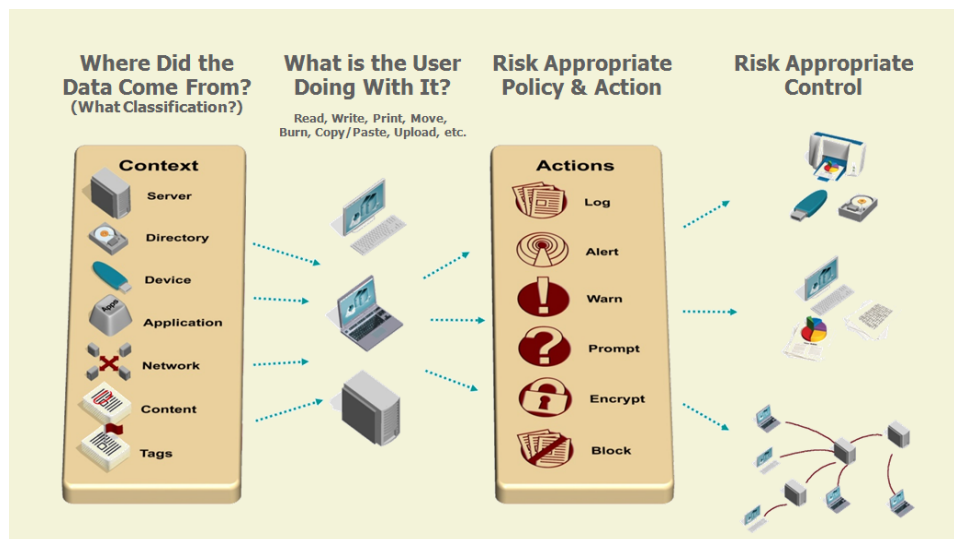
A typical, yet fairly critical example is the task of protecting passwords in a biometrics system. Many biometric installations are sited and managed by the real estate and facilities department of the company and not controlled by an IRM system. Employees that administer the biometrics system may leak passwords to outsiders. A network DLP system can prevent transfer of biometrics passwords on all channels regardless of user rights since it is independent of the IT infrastructure.

### 3. The technical aspects of a non-rights approach - agent DLP

In this section, we will review some basic technical aspects of agent DLP technologies.

Agent DLP technology is based on a light-weight, autonomous kernel level software agent running on the user workstation. The agent hooks into Windows system calls and detects policy violations as the user is performing an action on his PC. Policies are based on data content inspection, context (source/destination of the data transfer) and action (what the user is doing). Content inspection is agnostic to the type of document – e.g. the same text patterns will be detected whether in a PDF or a Microsoft Office document. Since the agent is autonomous, it can enforce policies on mobile notebooks that are off line from the network.

The agent can execute a number of security countermeasures in reaction to a policy violation - for example silent logging of an event to the centralized management console or automated encryption on demand if a sensitive file is being transmitted to an unauthorized destination such as gmail.



A central management server is used to configure a company-wide data security policy. The management server distributes agents to endpoints and collects alerts into an analytics database.

Data security policies can be controlled in a finely granular fashion from a single Windows domain user, or Active Directory group policy for all users.

The agent and its management server can trace a sequence of data flow operations and execute security controls such as alert, prompt or block, even when the first transaction was still permitted (for example copying a classified file from a Windows share (which is permitted) but posting to Facebook (which is not permitted)).

#### 4. What's important? Look for security, don't look for features.

Since the business situation, corporate culture and IT infrastructure of every company is different, we believe that it is incorrect to choose security countermeasures on the basis of product features – especially when vendors provide pseudo-risk-management justification for their offerings.<sup>2</sup>

Instead – we submit that selection of security countermeasures requires measuring their effectiveness against a particular threat. The below table provides a simple comparison between IRM, agent DLP and network DLP for the top 3 risk threats in a typical company.

Threat	Agent DLP countermeasure	Network DLP	IRM countermeasure
Trusted insider leaks information	<p>Install agent on every PC</p> <p>Define policy of content and context.</p> <p>Monitor, block, alert, warn, prompt, block.</p> <p>Execute policy everywhere – even when the PC is off the network</p>	<p>No software installations on PC. Network DLP appliance performs Level 2 content interception.</p> <p>Define policy of content and context.</p> <p>Monitor, block, quarantine</p> <p>Execute policy at the network perimeter or inside the data center</p>	None
Trusted outsider leaks information shared with a trusted insider	<p>Encrypt the data on-demand.</p> <p>Need agent at receiving endpoint in order to decrypt the data.</p> <p>Automated encryption on demand according to centralized policy. No key exchange required.</p>	None	<p>Need IRM client in order to access the information according the predefined rights schema.</p> <p>Requires the sender to opt-in to use the system, otherwise the document is sent in clear text.</p>
Malicious insider/outsider may exploit vulnerabilities in client software.	<p>Autonomous agent at endpoint protects data at the kernel level by intercepting Windows system calls.</p> <p>Not detectable as a running Windows service, not easily compromised or exploited.</p>	Immune to client side exploits	Data is protected at the application level and can easily be cracked <sup>3</sup>

2 Security Metrics, Replacing fear, uncertainty and doubt, Andrew Jaquith 2008. “Risk management is where the confusion is”, “The hamster wheel of pain” - pages 2-4

3 The self protection strength of DRM client software has always been a weakness for all DRM solutions, and application-specific implementation also restricts the deployment of many IRM systems. See Y. Yu and T. Chiueh “Enterprise Digital Rights Management: Solutions against information theft by insiders”

## 5. How to choose? Use the scientific method

Based on our internal security consulting experience over the past 5 years, a company must ask a series of questions in order to test two fundamental hypotheses:

*Hypothesis # 1: Information leakage is currently happening at a level justifying a capital investment in data security.*

- What are the data types and volumes of data leaving the network?
- Who is sending sensitive information out of the company?
- Where is the data going?
- What network protocols have the most events?
- What are the current violations of company Internet Accepted Usage Policy?

*Hypothesis # 2: A cost-effective set of security controls exists that can reduce risk to acceptable levels.*

- What are the top risk threats?
- What is the value of information assets on PCs, servers & mobile devices?
- What is the value at risk?
- Are security controls supporting the information behavior you want (sensitive assets stay inside, public assets flow freely, controlled assets flow quickly)
- How much do current security controls cost?
- How do you compare with other companies in your industry?
- How would risk change if you added, modified or dropped security controls?