



# SECLORE

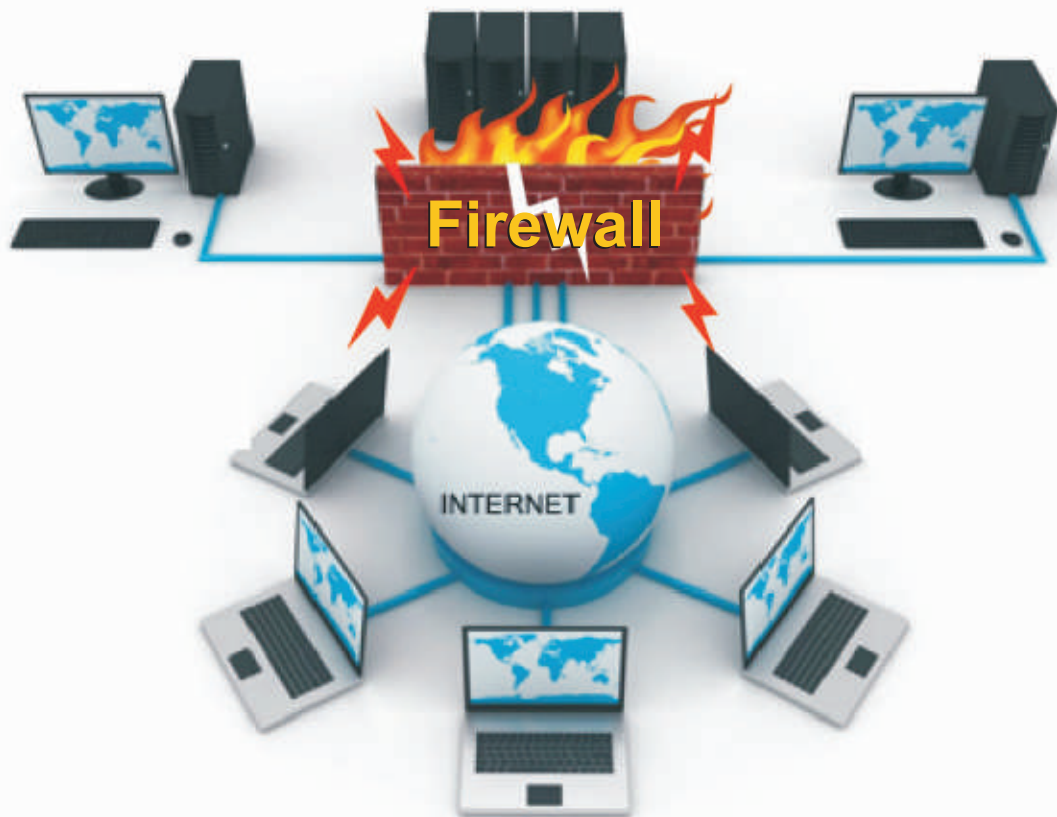
## Information Rights Management for Collaborative Businesses

A WHITE PAPER



## 'Social Engineering Bypasses All Technologies, Even Firewalls'

- Kevin Mitnick (*Founder Mitnick Security Consulting & Controversial Hacker*)



**Social engineering** is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

**INDEX**

|  |           |
|--|-----------|
| <b>Introduction</b>                              | <b>1</b>  |
| <b>Challenges</b>                                | <b>2</b>  |
| <b>Considerations for Information Security</b>   | <b>4</b>  |
| <b>Introducing Information Rights Management</b> | <b>6</b>  |
| <b>Remote controlling Information with IRM</b>   | <b>7</b>  |
| <b>Other Salient Features of IRM</b>             | <b>8</b>  |
| <b>Benefits of IRM</b>                           | <b>9</b>  |
| <b>Conclusion</b>                                | <b>10</b> |
| <b>Contact us</b>                                | <b>11</b> |

## Introduction

According to a study conducted by Ponemon Institute in 2006, data leaks damage businesses to the tune of \$ 4.7 million, wherein only 10% data leaks are caused by hackers. Almost 45% of data leaks were caused by transporting data out of authorized environments using mobile storage devices (PDAs, Mobile Phones, Portable Drives, Laptops). As businesses gear up to face new challenges of collaborative businesses, information security will be amongst the prime focus areas, and formidable Information Security Frameworks is required to complete the business eco-system in which enterprises and their business partners conduct business.



DILBERT@2009, UNITED FEATURE SYNDICATE, INC.

Security for Business Information has been the focal point of most CIO strategies. Competitive edge of organizations, regardless of the domains they conduct business in, lies in the intellectual properties (IP) that differentiate them from competition. While on one hand, IP needs to be guarded at all costs; on the other hand the emphasis on collaboration for businesses forces this information to be shared outside the confines of the enterprise. More often than not, IP is in the form of information, and resides in a multitude of places, including desktops, Document Management Systems (DMS), emails, shared repositories, files, documents, etc., within and outside of the organization. Traditional approaches for securing documents and the information within it tend to postulate that access control guarantees information security too. Also, most of the endeavors for information security are directed towards security within the boundaries of the enterprise. After the document has left the enterprise, providing dynamic security to it is regarded either too cumbersome or just impossible.

With the popularity of the Internet in business communities enterprise boundaries have become somewhat blurred. Also, in order to be agile, many sporadic decisions regarding information sharing become mandatory so as to gain a position of benefit in a business situation. At such times, an inflexible information security infrastructure could obstruct the path to success.

This whitepaper attempts to highlight considerations that, amongst others, need to be part of the enterprise-wide information security initiatives, so as to enable enterprises to be ready to face the challenges of secured information sharing in the 21<sup>st</sup> century, and beyond.

## Challenges



### *The enemy is outside... so is your information!*

Most information security measures like network firewall, VPN networks, token-based authentication are perimeter-centric security systems. At the lowest level, they provide security against unauthorized access from outside of the enterprise perimeter. But often, business information such as contracts, price sheets, etc. are required to be sent to vendors, business partners and prospective/existing customers for their own consumption.

In such cases, sensitive information is sent out of the enterprise boundaries, with absolutely no control to ensure that the information is not intentionally or accidentally accessible to unintended people.



### *The enemy is inside... so is your information!*

Stakeholders within the enterprise are provided access to specific sensitive information so that they can carry out their official responsibilities and for the purpose of collaboration. During the time a person is an employee of the company, IP available to him/her could have possibly been transferred onto personal storage devices. The stakeholder would probably have all this information available to him even after his association with the company ceases.

In another case, stakeholders have a lot of personal and corporate confidential and sensitive information on their laptops and removable media (CD, USB drives, etc.). In case these devices get stolen, the thief has complete access to the information on the device.

## Challenges



### *It's All or Nothing... there are no grey shades*

The options available and considered by CIOs for information security tend towards access control. Often, for security purposes, either access is provided to information or not. There are very few options, if any, to provide usage rights to information. A business situation may warrant providing read-only rights to some, printing rights to others, and edit rights to some. Also, even if a person has read-only access to information, it is possible for him to edit the newly created document, and claim it to be the original. The security rights do not affect the new document, as it is considered a different one. The only way to prevent this currently is to restrict access to the information completely, which in-turn would restrict collaboration required to do business under various circumstances.

The above case brings us to the well known fact amongst the IT Security community that “Security and Collaboration are two sides of a coin.” One suffers at the cost of the other.



### *Different strokes for different blocks*

Blocks of sensitive information reside in different places within the enterprise. While some may be in the form of documents, some could be on websites, and others could be in the form of images and drawings. Usually different security frameworks would be adopted to protect different forms of information, and possibly each offering different levels of maximum security.

In this case, the total cost of ownership for information security increases significantly for CIOs, while often providing lesser than required security across all quarters. The sum of parts is lesser than the whole.



### *Protection only within*

Content repositories like Document Management Systems (DMS), Content Management Systems (CMS), Core Banking Systems (CBS) have complete control on information when they are within their perimeter. But once the information leaves the gates of Content Repositories by means of a download, the Content Repository loses its controlling authority. Thereafter the information can be freely distributed, edited, printed by not only the user who has access to the Content Repository but also by anyone else.

## Considerations for Information Security

The need of the hour is to provide a location and system agnostic, granular and flexible information security framework. Some of the considerations for such a system are discussed below:



### ***Persistent End-to-End Protection***

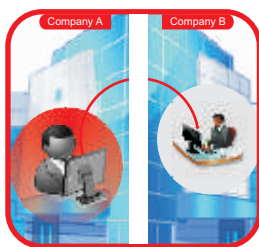
Information traverses through a lifecycle of creation (IRM), storage (folder/disk encryption, IRM), transmission (DLP, secure protocols, IRM) use (DLP, IRM) and deletion/archival (encryption, secure storage, IRM). A robust information security framework should provide adequate protection across all these stages of the information lifecycle. The information should be protected at anytime and at anyplace even if it is outside of the enterprise boundaries.



### ***Access Control v/s Usage Control***

Businesses today need more than just traditional security provided via access control by most information security endeavors. Security should be provided on the usage of information and not restricted to access only. Different class of consumers of information should be allowed selective usage of the information.

It should be possible for the owner of the information to decide and imply not only who can view the information, but also, who can do what with it, and possibly from where. For example, a document may be printed within the confines of the enterprise, but may only be read-only if accessed from outside. Complete flexibility should be available to the owners of the document to entail who can perform actions like view, edit and print on the information. Also, it should be possible for the owner to allow this on the basis of time periods.



### ***Static Control v/s Dynamic Control***

Traditional security solutions like password protection only provide static control on information. The controls that are put on the information cannot be changed thereafter. Given the pace at which business relationships between organization and employee; organization and vendor; organization and client changes, there is an absolute requirement to be able to remotely and dynamically change the permissions that a user has on the information. At times, there is a need to even remotely destruct the information that is residing on the defaulters' computer.

## Considerations for Information Security



### **Online and Offline Protection**

While the percentage of time spent online while doing business is increasing, it is far from being 100%. A substantial amount of business activity is still performed when no connection to the internet is available, while being on the move or from home. For all such activities, access to secured business information is required. Information access could be online as well as offline, depending on the business conditions. Information security should be enforced regardless of the consumers' online status.



### **Compliance**

Recognizing the significance of information security, various regulatory bodies have imposed standards compliance, to ensure information security is enforced. ISO 27000, BS7799, Sarbanes Oxley, HIPAA, etc. all tend towards enforcing Information Security with different focus areas or business domains. An information security framework should comply with the requirements of most, if not all, of the prevailing security standards. Requirements such as, but not restricted to, Audit Control and tracking on authorized as well as un-authorized attempts to access documents, ability to map business contexts to security levels, etc. should be well supported. This will help in further supporting the organizations endeavor to be certified, compliant with specific regulatory bodies.



### **Completing the loop**

Apart from the above, adequate support should be provided in other matters, to address information security requirements for various business requirements. Support for all popular file formats, possibilities to integrate with existing business systems (like Document Management, Workflow, ERP) and Active Directory (or other LDAP-based Directories), role-based rights management assignment, etc. should be matted with the base security offerings to make administration easier and usage more flexible.

## Introducing Information Rights Management (IRM)



Uncontrolled replication and distribution of information over a ubiquitous medium like the Internet is very easy and ultimately translates to revenue and competitive advantage loss. IRM technology (like the ones offered by Seclore, Microsoft and Oracle), enables an enterprise to enforce usage control policies such that all digital assets of the enterprise, within or outside of the corporate firewall, exchanged between employees and between the organization and vendors/clients is protected persistently at all times, irrespective of the location.

IRM technology enables “owners” of information to control the actions that are performed on the information once it has been distributed. IRM protects the information and restricts usage to only specific users or groups, specific actions like view, print, edit, copy content and distribute, specific time of usage like “till 19th August 2009” or “2 days”. With some IRM technologies, the owner of the information can also restrict the usage to specific computers and network IP addresses, thus providing one more additional layer of control when giving access to systems outside of the organization.

These controls are applied to the content itself without any constraint on the computer, network, storage or transmission technology used. In most cases, the controls are also dynamic. For example, if the “owner” wants to change the controls to provide usage to a different set of people, different set of actions, etc. it is possible for him/her to remotely change the rights to all copies of the information which have already been distributed. One of the core benefits of IRM technology is that it implements security and control irrespective of the location of the content within or outside of the enterprise.

## Remote Controlling Information with IRM

Protecting information with IRM involves manually defining “usage rights” for the information before it is distributed. Some IRM technologies also provide the flexibility to define policy templates for protection. Advanced IRM solutions provide automatic classification of information based on the content, meta-data etc and automatic protection depending on the classification.

**The usage rights are a combination of the following controls:**

**WHO can access the information:** This typically relates to a user repository like an LDAP system and also maps the organization hierarchy of users, groups and organization units. With some IRM technologies, it is also possible to link this to non LDAP user databases as defined in custom applications and portals.

**WHAT can each user do with the information:** This typically relates to individual actions allowed on the information by the specific user. Individual actions which can be controlled are viewing, editing, printing, forwarding/sharing, copy/paste of content and unprotecting.

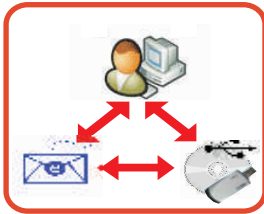
**WHEN can each user access the information:** This control can limit users to access the information within a specific date range or time span. A document could thus have “19th August, 4 pm to 23rd August, midnight”, as a specific date range or “2 days from first access”, as the specific time-span within which the document is available.

**WHERE can the information be used:** Even within IRM technologies, this is not-so-commonly available feature which could become useful in cases of information of extreme confidentiality. This control can restrict usage of the information to only a pre-specified list of computers identified by the hardware or to a specific range of IP addresses or networks.

In most cases the above usage rights are seamless and transparent to the end user. The user's experience, as long as his actions are permitted by the system is also exactly the same as before.

## Other Salient Features of IRM

Apart from the above control features, IRM provides a lot of other features. Salient features are:



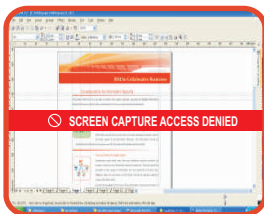
### 1. No restrictions on method of information distribution

Document distribution can happen through existing channels like email, CDs, fileshares, etc. Hence, there is no change in the existing way of working and collaboration.



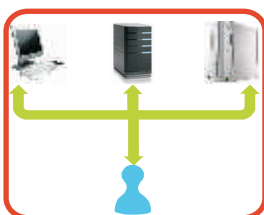
### 2. Support for "Offline" usage

This feature is primarily for mobile users. It provides the ability to view the document even when the user is not connected to the network.



### 3. Prevention of screen capture

Advanced IRM solutions, control screen grabbing through "Print Screen" as well as screen capture tools like Snag-It, remote desktop sessions and online meeting sessions. This prevents data leakage and ultimately revenue loss.



### 4. Multiplicity of clients

Documents can be protected from within the desktop or from server or any other central repository of documents.



### 5. Full audit of authorized activities and unauthorized attempts on the document within and outside the enterprise:

Central availability of the audit trail of all activities on the document ensures that deviations can be caught early on as well as compliance to regulatory frameworks is easy to ensure.

## Benefits of IRM



IRM technology brings tremendous security and benefits to the organization by preventing information loss. IRM provides complete and persistent usage control on information throughout its life cycle of creation-distribution-use and destruction. With IRM, security can be ensured without compromising on the why users collaborate.

One of the major benefits of IRM is its audit trailing mechanism. IRM can audit trail the usage of the information

from the time it is protected. All authorized actions as well as unauthorized attempts are logged, tracked and reported. The granular details of *Who* did *What* with the information from *Where* and *When* was the attempt performed can be tracked and reported. This helps organizations to adhere to regulatory and compliance frameworks like ISO 27000, Sarbanes-Oxley and HIPPA, for “unstructured” data control. It also helps to detect any suspicious activities that are going on with any information. For example, the system can be setup to send an alert if there are three print requests on a document within a time span of five minutes from a particular location.

IRM can also significantly lower costs and process delays associated with version control and document retention policies. With IRM, information can be shared with employees and business partners with no large additional investment in security systems. It increases revenues by preventing misuses, theft and leakage of content.

## Conclusion

IRM is well positioned to satisfy today's increasing enterprise needs for regulatory compliances with standards such as BS 7799, Sarbanes Oxley, Gramm-Leach-Bliley, HIPAA, and the like. Mandates for appropriate usage of sensitive information by any employee, contractor, consultant or partner can be enforced and adhered to persistently in the information lifecycle and in all possible applications and workflows to completely eradicate information leakage. An enterprise can hence stay in compliance all the time easily and consistently.

## About Seclore

Seclore Technology is a high growth security software product company, providing security solutions in the areas of information usage control, Information Rights Management (IRM) and secure outsourcing.

Seclore's expertise lies in the control of information post distribution, irrespective of its location and mode of transfer. With this the receiver is able/not-able to distribute, edit, print, copy-paste, screen-grab information from the document. It is also possible to remotely destruct the documents at the receivers end.

Some of the largest companies in banking and financial services, insurance, engineering services, educational institutes, among others, use Seclore's technology to secure data that is used internally or provided to a vendor for outsourced processes.



## SECLORE

Call: +91-22-4015 5252

[info@seclore.com](mailto:info@seclore.com)