Securing Intellectual Property across the internet by Integrating Data Classification with Digital Rights Management

Rick Orloff

GIAC Security Essentials Certification (GSEC)

Version 1.4b
Option 2

March 5, 2004

Introduction

The purpose of this document is to define a process to mitigate the risk of sending electronic documents across the internet to customers, suppliers, vendors, and all third parties while providing a secure solution that supports business unit needs. Managers and IT professionals can utilize this document as a framework to understand the value of integrating data classification with Digital Rights Management (DRM). For example, if your company produces significant amounts of intellectual property, there is often a business need to collaborate using softcopies outside the Enterprise. DRM creates a balance between security controls and risk management.

For the purpose of this paper, the definition of a secure document has three requirements:

1. Only intended recipient(s) can access a secure document even after the document has left the corporate domain and resides on someone else's personal computer.
2. The sender retains the ability to control the Edit, Copy, Save, Forward, Print, and Time to Live, permissions to the secure document even after the document leaves the corporate domain.
3. The sender retains the ability to revoke access to all previously sent documents.

Assumptions:

- The Enterprise is global.
- The corporation has embraced an "outsourcing" strategy.
- The company has R&D with Intellectual Property in constant development.
- There are regulatory requirements effecting different business units.
- Corporate governance wants strong internal business controls.
- The Information Security Manager likes cool solutions. (Note: The CIO believes this item is a Problem Statement)

PROBLEM STATEMENT

Within outsourcing models, business partners, and supply chain management, we send electronic copies of Intellectual Property (IP) without strong security controls, IP protection, or audit abilities. Frequently, we rely on the recipients internal business controls, contractual obligations, and individual ethics, however any or all of these factors may not be sufficient to protect our Intellectual Property from misuse. Frequently, our intended suppliers will share our drawings and other IP with their own supply chain, or "third party suppliers" that we have no relationship with. This means our documents are being distributed without our approval, control, or audit mechanisms.

"…perimeters are dissolving as they "extend" their enterprise to their partners, suppliers and customers by sending them confidential company information…"
Sealed Media Corp

Securing corporate assets and intellectual property should be constructed with a Defence In-Depth or layered, approach. Security should include physical controls, network security controls, and controls of data; based on the data's importance to the company. True document control means we should be able to acquire a synchronous audit trail as well as revoke access to the document no matter where it resides. We cannot truly protect against accidental or malicious digital leakage of intellectual property unless we can also attach controls to the data itself. In this manner, the controls extend to all sorts of media including CD, DVD, Floppy, Flash, etc.

Network Security

Although we often apply security to the seven layer OSI model, we too often lose control of our data outside our own domain(s). Here is one scenario of a corporate document being accessed:

User authenticates onto the network, has access to the document (data), transmits (Layer 5 20/21/25) the document to a vendor (collaboration), and from there, auditable Information Security controls stop. At this point, our Information Security controls are solely civil based controls such as Non-disclosure Agreements (NDA) or contracts. The difference is such devices are not true control but legal agreements and remedies. Moreover, the OSI model doesn't necessarily enforce a corporation's data classification or document control outside its own domain.

This is analogous to having a family policy stating that your eight year old is not allowed to eat the candy bar in his backpack until lunch time at school. It's probably a good rule that even a nutritionist might consider "best practice" but the policy can't be enforced or audited. Additionally, it doesn't prevent the eight year olds younger brother from taking it (a.k.a. liberation of a candy bar) before school starts.

Most existing corporate data security plans focus their efforts on network perimeter protection, firewalls, and unauthorized access instead of focusing security on the data attributes itself. Such processes do not prevent accidental or malicious leakage of information and fail to enforce an organization's document classification policy and procedures. A typical domain will have a series of defence mechanisms including, but not limited to:

- Firewalls
- Authentication schemes
- Virus Scanners
- IDS
- Public Key Infrastructure, PKI
- File and Email encryption, such as s-mime and/or PGP

Figure 1.0 illustrates typical scenarios for communications to outside corporations from a network. The “red dot” is characterized as an Information Security Control Point.

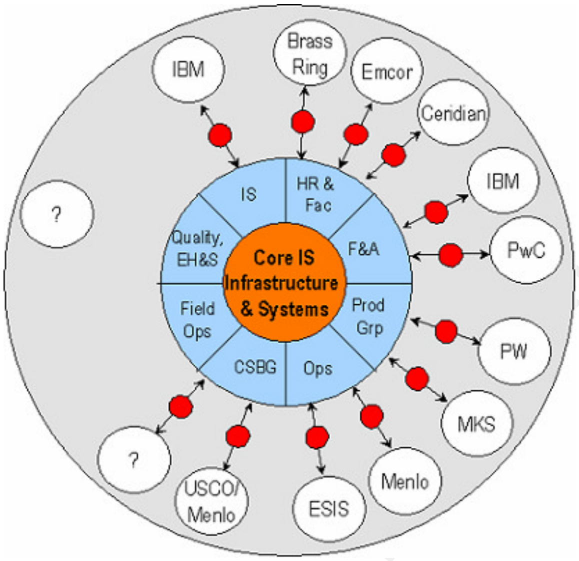


Figure 1.0 Information Security Control Point

Regulatory Requirements

As part of SOX 404. AB1386, HIPPA, and U.S. Department of Commerce, we need an Information Security program that allows audit ability while still being flexible enough to adapt to new or evolving standards. For example, if in two years the Department of Commerce changes their definition(s) for controlled export of our products to address advances in technology, a well planned Data Classification scheme integrated with matching information security controls would allow the corporation to simply reclassify, or shift the scale providing audit ability of the new controls with minimal administrative effort.

“Beginning July 1, 2003, SB 1386 requires companies, non-profits, and government agencies that conduct business in California to notify their California customers when their personal data is compromised due to a computer security breach”

Guidance Software - The Leader in Computer Forensics & Incident Response Solutions

Email Attachments

In most networking environments, there is a natural assumption that when email attachments are sent outside of the network, the sender losses control of the document. Any recipient of the document can copy, forward, print, etc. Generally, this is when corporations are forced to rely solely upon Nondisclosure Agreements (NDA), contractual obligations, corporate governance, or even the individual recipients’ core values to protect the intellectual property from unwarranted disclosure. There are several solutions available to address this unintended document distribution or “Digital Leakage.”

Two different approaches are to secure the delivery or payload through a Secure Socket Layer (SSL) connection or to place security controls on the payload itself. Setting up the SSL connection is relatively straight forward; however, the question remains how to continue security of the payload after delivery. Recall that our definition for security meant that the recipient(s) couldn't edit, copy, forward, save, or print the document unless we authorized them to do so. Moreover, the document has a Time to Live (TTL) defined making it unreadable after a preset date and/or time. This is truly the Mission Impossible version of self destructing documents. It will literally disappear from the screen if expired. Although it continues to reside on the storage media, it remains in an encrypted state. The methodology for this is known as Digital Rights Management (DRM).

For a secure SSL email delivery solution, there is Tumbleweed's (www.tumbleweed.com) Secure Redirect product, a very effective server that can be utilized to encrypt delivery across the session layer with HTTPS. Additionally, it is account based and has audit controls. For many companies, this level of security is sufficient. Our concern is this didn't provide the desired security and usability of documents post delivery.

There are several Digital Rights Management (DRM) solutions that can be utilized to secure documents post delivery. The DRM solution we found to be most effective was from Sealed Media (www.sealedmedia.com). DRM can be described as wrapping a 128bit digital certificate around a document. Afterward, the sender controls the rights to the certificate.

Viruses

Several viruses in the past emailed data files from users machines without the user's knowledge or consent. Publicly traded companies or pre IPO companies can suffer irreparable damage. U.S. based companies may further be impacted by statutory or regulatory controls that may have serious financial penalties while others have provisions to incarcerate the Information Security Officer. With DRM, any unauthorized access to data files still leaves the data in an encrypted state accomplished via a 128 Bit Asynchronous Key.

DATA CLASSIFICATION

Figure 2.0 below (followed by definitions) depicts a three layered data classification scheme. The scheme better enables a corporation to achieve Return on Investment (ROI) by focusing its security and infrastructure expenses on the most valuable data for the company. Without distinguishing our data, we are in effect requiring all of it to have the same level of security. This does not have an efficient ROI based on expended dollars compared to the value of data protected.

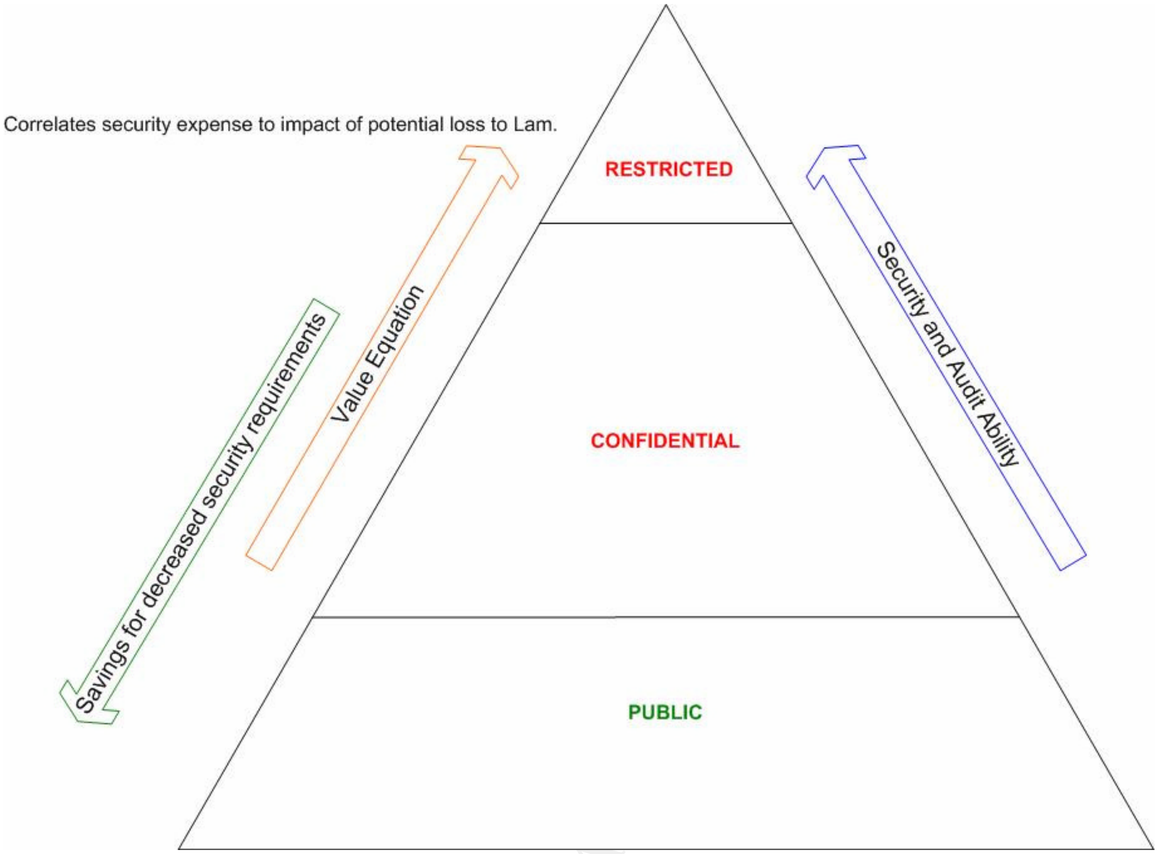

Correlates security expense to impact of potential loss to Lam.
RESTRICTED
CONFIDENTIAL
PUBLIC
Value Equation
Savings for decreased security requirements
Security and Audit Ability

Figure 2.0 Data Classification Scheme

Below are proposed definitions for the three level classification scheme illustrated above. The definitions themselves are guidance to data owners. If data can be classified under more than one category, the most restrictive classification must be applied.

RESTRICTED: This classification applies to the most sensitive business information which is intended strictly for use within the company. . Its unauthorized disclosure could seriously damage the company, its banking relationships, reputation, competitive position, business partners, and/or its customers. Guidance for this example includes:

- OLT, CEO and Board of Director information
- Research and development data
- Product development
- Highly sensitive information about strategies, plans, designs, mergers and acquisitions
- Litigation strategy memos
- Intellectual property and patent information
- Revenue forecasts and all financial data
- Information relating to networking resources including but not limited to infrastructure design and passwords
- All trade secrets

CONFIDENTIAL: This classification applies to less sensitive business information which is intended for controlled use within the company. Its unauthorized disclosure could adversely impact the company, its banking relationships, business partners, its employees, and/or its customers. Guidance for this example includes:

- Unpublished market research
- Strategic alliance agreements
- Work in Progress
- Internal corporate documents not classified as “Restricted”
- User account passwords
- Internal audit reports
- Employee information
- Organizational structure and/or changes
- Policies and Procedures
- Customer information
- Activity occurring under Nondisclosure Agreements (NDA)

PUBLIC: This classification applies to information which has been explicitly approved by company management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Note: It is the responsibility of the ***owner or the originator*** of the information to classify it appropriately and to restrict its distribution to the intended audience. Senior Managers and Executives of the company should offer advice to individuals in this respect.

Policy and Procedure

After deploying a data classification throughout the enterprise, the next step is to utilize DRM to secure the data. One way to look at this is Data Classification is your “policy” and DRM is part of your “procedure” and security controls.

DIGITAL RIGHTS MANAGEMENT (DRM)

What is DRM and how does it work?

The significant value of DRM is a perfect textbook deployment of network protection with a Defence In-Depth approach provides hardening of the OSI layers but does not provide security controls for the soft gooey centre we call our data when it needs to be communicated outside the network.

It simple terms, DRM utilizes a 128bit digital certificate and "wraps" a document with the cert to provide security attributes to the certificate itself. The sender, or other internal triggering process, assigns permissions to the certificate for access control and audit ability; such as who accessed, annotated, or attempted to print copy, forward etc. SealedMedia's (www.sealedmedia.com) diversity in the number of document formats it supports as well as the granularity of assigning permissions were the determining factors in selecting the solution deployed on our Enterprise.

SealedMedia utilizes a "Sealer" and "Unsealer" which are browser plug-ins; compatible with both Internet Explorer and Netscape. The sender has the rights and permissions to seal documents and the recipient only has the ability to unseal their own documents but can be granted additional permissions. The plug-ins (Sealer and Unsealer) both talk to a SealedMedia license server sitting in the DMZ. This is where the granular control occurs.
Figure 3.0 demonstrates a basic deployment.

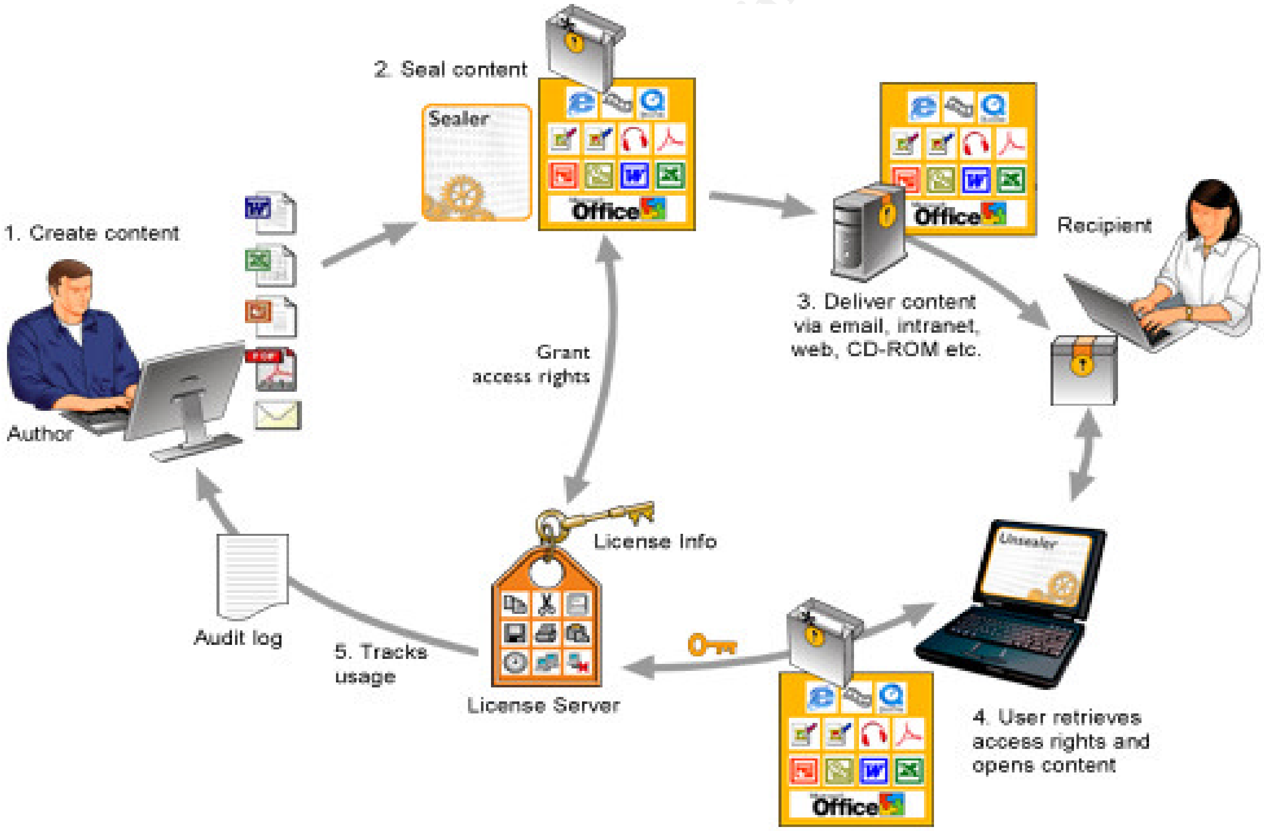


Figure 3.0 provided by SealedMedia

Figure 3.1 depicts several features, or settings, that can be used to control softcopy documents.

Copy	Sender decides if recipient is allowed to copy the document, or not.
Forward	Sender decides if recipient is allowed to forward copies.
Print	Sender decides if recipient can print copies and if so, can limit the number.
Save	Sender decides if recipient can save the document or have it as 'view' only.
Time to Live (TTL)	Sender decides how long the document is available to the recipient.
LAN v. Offline	Sender decides if the recipient can view document offline.
Delegation	Sender can delegate rights (similar to Active Directory).
Revocation	Sender can revoke access privileges to previously sent documents.
Audit	Sender can audit when recipients received, open, or printed a document.
Watermark	Sender can require user identification imbedded on printed documents.

Figure 3.1 Permissions Table

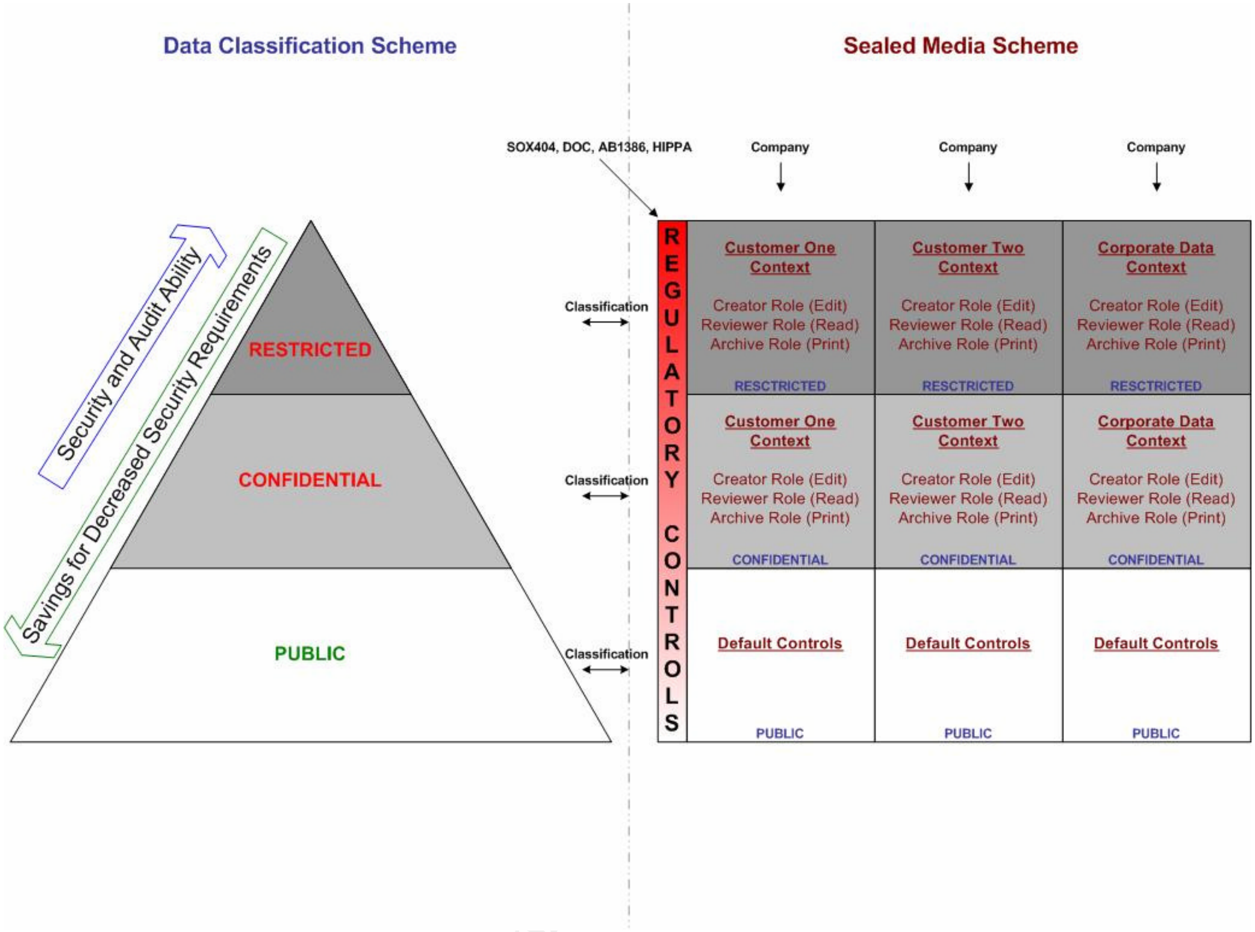
Audit Abilities

Data custodians, basic users, and security management each want different levels of audit capabilities. While a basic user might be satisfied with receipt type information, a data custodian may desire greater detail such as what was edited, what was printed, by whom and when. The Information Security (Control Nut) may want still greater granularity that can withstand forensic scrutiny in a court of law Details available about the end user include user credentials, machine name, as well as IP address

Audit details are available in real-time, and as a triggering event. Offline users continue to have their activity audited with the detail transmitted back to the license server when they are online. Note: Making files available offline is optional. Data owners or Security Managers may choose to be notified by SMS messaging or email if a particular file is opened, or access was attempted. Notifications can be mapped to a corporate data classification scheme or be done on an add hoc basis.

DRM Integration

Figure 3.0 below illustrates how a data classification scheme and a digital rights management program would be integrated to provide security controls and audit ability for Customer, Company, and Personal data residing on our network.



Customer One Context	Customer Two Context	Corporate Data Context
Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) RESCTRICTED	Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) RESCTRICTED	Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) RESCTRICTED
Customer One Context Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) CONFIDENTIAL	Customer Two Context Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) CONFIDENTIAL	Corporate Data Context Creator Role (Edit) Reviewer Role (Read) Archive Role (Print) CONFIDENTIAL
Default Controls PUBLIC	Default Controls PUBLIC	Default Controls PUBLIC

Practical Applications

Before deciding on a secure transmission and control strategy for documents, we need to define what we want to secure and why:

1). Research and Development (R&D) can collaborate internally and externally with tightly controlled documents. Towards the end of the R&D phase, companies prepare to file new patents and the legal department may need to collaborate with the development group as well as outside legal council specialists in filing patent applications. Not surprisingly to InfoSec specialists, many law firms don't have sufficient security for electronic documents. Moreover, law firms may use other third party resources that require softcopies of corporate IP. This means more copies of legal documents, future patent filings and other legal correspondence are being circulated then we could possible know about or ever wish to authorize.

Even worse, experience has indicated that some third parties go as far as to send future patent filing documents to their own AOL and Hotmail accounts so they can more easily work at home.

2). A corporation would have the ability to control distribution, or revisions, of documents to its employees with assurance that the document cannot be redistributed in an unauthorized form. For example, a memo from the CEO might be allowed to leave the network. Additionally, a document such as a technical memo could effectively be recalled if it contained errors or was out of date. The restrictions can even be applied retroactively so access is only allowed to the most recent version.

3). We want access controls to align with a corporate data classification scheme in order to provide access to corporate data in a secure fashion with minimal user impact.

4). Some corporations have transitioned to an "outsourcing" model in an effort to shift from Capital Expenditures to Operating Expenditures. Unfortunately, not all network configurations such as a large closed network, adapt themselves to an outsourcing model as quickly as the corporation would like.

As part of the outsourcing model, many contract companies and employees will need to authenticate onto the network. Part of the problem is that not all infrastructures or topologies have robust "role based" access controls. This means users authenticated on the network frequently can gain access to high-level data which is completely unrelated to their job function. This includes corporate IP, salary information, financial reports, executive directories and a myriad of other sensitive information.

CONCLUSION

Network managers are being increasingly tasked to provide connectivity to third parties while continuing to address increasing regulatory controls. Balancing a secure delivery solution such as Tumbleweed's Secure Redirect product with Sealed Media Digital Rights Management solution provides depth in secure delivery of data or email. In part, security solutions balance risk management with a recipients need to know.

While Tumbleweed provides a secure delivery solution with easy to use triggering points that can be integrated with other systems, Sealed Media continues securing data post delivery. The balance of the two can be cost effective while serving different business unit needs.

If we focus on regulatory controls many of us have to address, we need a security program that adapts to changing definitions of the controlled data. For example, in the semiconductor industry, some of the technology can be classified as munitions requiring regulatory controls to some foreign countries and/or foreign nationals. As the industry moves through technological advances, today's controlled technologies (classified as munitions) eventually become outdated and may be freely exported to previously restricted countries.

This means we need a data classification scheme with security controls that provide scalability with minimal administrative effort. Conversely, if we look at what occurred with Sarbanes-Oxley and HIPPA, previously existing data frequently spread across an enterprise network suddenly needed to be classified and protected while still exchanging the data with the intended recipients. In both scenarios, the data requires strong security controls with audit ability. Moreover, the laws requiring the controls have provisions for incarceration (prison time) for failing to meet the obligation. Of course, this might require some negligence of the security and corporate officers involved. Either way, I seem to recall reading somewhere that I'm not supposed to allow myself to be incarcerated although that can be Darwin's natural "fight or flight" syndrome taking effect.

In the US, it may not be sufficient to have contracts, nondisclosure agreements, and civil remedies available. When it comes to the U.S. Department of Commerce Foreign Trade laws, the ownership and responsibility for the data resides with the originating company and not necessarily the entity that has a copy. In comparison, many of the other regulatory requirements segregate the responsibilities and focus on authorized copies of the data. If we apply a best practice security model to the most restrictive requirements, we will maintain compliance and scalability.

With the current need to conduct business in a global economy, integrating data classification with digital rights management provides the ability to provide data files to persons that have a need to know, take it back when they are done, as well as maintain audit ability.

LIST OF REFERENCES

Sealed Media Corporation, Deployment Architecture
www.sealedmedia.com

Tumbleweed Communications, Secure Redirect,
http://www.tumbleweed.com/en/products/secure_redirect.html

U.S. Security & Exchanges Commission, Sarbanes-Oxley,
http://www.sec.gov/spotlight/sarbanes-oxley.htm

Guidance Software - The Leader in Computer Forensics & Incident Response Solutions, Assembly Bill 1386
http://www.encase.com/corporate/press/2003/20030414.shtm

Pro-TecData, Naomi Fine – Data Classification
http://www.pro-tecdata.com/naomi/

Sync Cast, Digital Rights Management for e-commerce
http://www.synccast.com/services/default.asp?page=drm

The near Future of Digital Rights Management, by Daniel H. Steinberg
http://www.macdevcenter.com/lpt/a/2768

China Information Security – A June 1999 report from the US Embassy Beijing
http://www.fas.org/nuke/guide/china/doctrine/infscju99.html

Information Security in Cyberspace: Emerging Legal Security Risks in Electronic Commerce
http://legalnet.com/Presentations/Info%20Sec%20Reg/webcast1[1].ppt

Don't Get Blindsided by Privacy and Security Regulations, by Richard DeLotto
http://www.gartnerg2.com/research/rpt-0102-0001.asp