



January 7, 2010

# Getting Data Protection Right

Combining the Counterintelligence Security Model with  
the Enterprise Rights Management Technology Platform

David F. Drab, CISSP  
Director of Security



**Sitrof Technologies, Inc.** | [www.sitrof.com](http://www.sitrof.com)  
Bringing It All Together  
Documents, Processes and People.  
Princeton | San Francisco | London | 866.545.8954 v | 866.422.9789 f

**Document:** White Paper

**Title:** Getting Data Protection Right: Combining the Counterintelligence Security Model with the Enterprise Rights Management Technology Platform

**Topic:** Information Security Management

<b>INTRODUCTION</b> .....	3
<b>THE PROBLEM</b> .....	4
<b>GETTING DATA PROTECTION RIGHT</b> .....	6
<b>STRENGTHENING SECURITY MANAGEMENT WITH THE COUNTERINTELLIGENCE MODEL</b> .....	6
<b>THE EMERGENCE OF ENTERPRISE RIGHTS MANAGEMENT</b> .....	7
<b>WHY ENTERPRISE RIGHTS MANAGEMENT?</b> .....	8
<b>HOW DOES ENTERPRISE RIGHTS MANAGEMENT WORK?</b> .....	9
<b>BRINGING IT ALL TOGETHER FOR SECURITY, COMPLIANCE, OPERATIONAL EFFICIENCY</b> .....	10
<b>CONCLUSION</b> .....	11
<b>ABOUT SITROF TECHNOLOGIES</b> .....	12

# Getting Data Protection Right: Combining the Counterintelligence Security Model with the Enterprise Rights Management Technology Platform

## Introduction

Your data may be secure when it is at rest or in storage...

Your data may be secure when it is in motion inside and outside the enterprise...

### **But is it secure when it is in use by an authorized user?**

If you can guarantee that your data is only being used for authorized company business—congratulations! We applaud your success. But if you are like most companies, you do not know this for sure. Data breaches are occurring with greater frequency and impact than ever before. A single breach of Personally Identifiable Information (PII) or ‘trade secret’ intellectual property could cause egregious harm to corporate brand and reputation and cost millions of dollars in remediation, competitive loss, legal fees, and regulatory fines. A 2009 Ponemon Institute survey revealed that 59% of ex-employees admitted to stealing confidential company information.

Enterprises today need to have a keen eye on human resources—the people within the chain-of-trust and the critical information assets that they create, manage, or otherwise have access to during the course of their employment. Information technologies and security innovations must come together to form a combination that delivers business intelligence for strategic decision-making. Security policies and procedures must be in place to manage activities, both online and offline, for every individual within the chain-of-trust.

Incorporating the principles of counterintelligence into enterprise security management provides many benefits. Enterprises today are without borders and security must be holistic, comprehensive, and strategic in focus. Complementing this approach is an innovative technology platform that offers unique functionality that provides:

- Dynamic, role-based policies for granular control over ‘who’ may access data and ‘what actions’ they may apply to the data once access has been granted
- Real-time visibility into data flows
- Real-time monitoring of end user activities
- Robust auditing
- Segregation of duties in security administration and oversight
- Strong cryptographic controls to protect confidentiality

Solutions today must help keep insiders honest whenever they walk out the door. After all, in the new information economy, security is really about making trusted-insiders trustworthy. This end result is what we call ‘persistent’ security for unstructured data. You cannot afford to let your mission critical ‘proprietary’ or ‘privacy-protected’ information leave the office without it.

***“Your sensitive data is walking out the door with your employees. Even if layoffs are not imminent, companies need to be more aware of who has access to sensitive business information.”***

Larry Ponemon, Chairman and Founder, Ponemon Institute, LLC

## The Problem

Your unstructured data and documents represent a treasure trove of ideas, innovation, and customer sensitive private information that flows in and through the enterprise as customer lists, marketing plans, product plans, financial models, research and development, human resources compensation plans, and privileged legal information. This kind of information provides a competitive advantage and can be protected under the law as a trade secret, if properly identified and managed. As stated in the Sarbanes Oxley Act, trade secrets are financial assets, which means if they are lost, stolen, or compromised a 'material change' has occurred, which requires that investors and shareholders be notified. They have a right to know.

Similarly, when privacy-protected information is stolen or compromised, another major problem arises due to the fact that much of this information is protected by federal and state regulatory laws. If you are in charge, you are accountable.

Information security management is a serious business mandate. It is a moving target, driven by business innovation and threat innovation. In this world of rapid change, we are seeing an unprecedented distribution of the enterprises' intellectual property and information assets. Compounding this are the escalating demands of citizens, consumer groups, and government legislators for dependable security. In other words, get information security right.

With these issues in mind, consider these questions:

- Has your organization implemented measures to build control and accountability around unstructured data that resides in documents stored in File Shares, Content Management Solutions, desktops, laptops, and email?
- Do the measures provide protection against theft by insiders with opportunity or malicious intent?
- Do the measures assure compliance with regulatory laws?
- Do the measures hinder or improve use and operational efficiencies?

These are important questions that must be asked when formulating a holistic security solution. Mission critical information is the engine of productivity, profitability, and competitive advantage. It is worth protecting!

Studies continue to reveal that unstructured data represents up to 85% of a company's overall data, and more than 50% of it is sensitive or mission critical. Unstructured data refers to hundreds of data types stored in documents such as: Adobe PDF, Microsoft Word and PowerPoint files, emails, instant messages, web pages, still images, scanned documents, audio files and video files. These data formats are multiplying rapidly, as is the volume of data contained in these formats. In a recent survey by the Aberdeen Group, 86% (nearly nine out of ten respondents) reported a year-over-year increase in unstructured volume, and an additional 46% reported a year-over-year increase in the number of collaboration and content management systems, such as Microsoft SharePoint and EMC Documentum.

The vulnerabilities resulting from the mismanagement of unstructured data is only one of two key factors in the enterprise information security equation. The other factor has to do with people, which often gets eclipsed by techno-centric solutions.

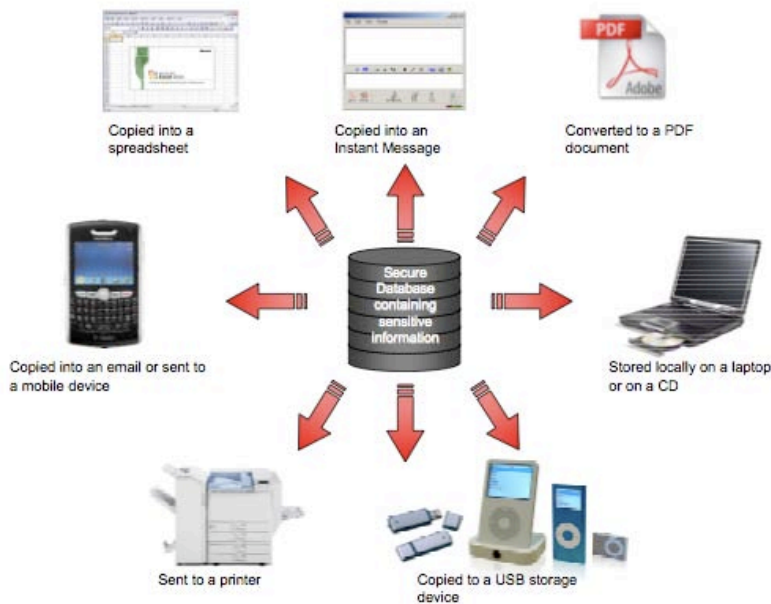
With employees and end-users in mind, consider these questions:

- Are controls in place to ensure that only persons with a need to know have access to sensitive data, information or content?
- Are controls in place to ensure that your data is being handled in an authorized manner and pursuant to policies and procedures?
- Does your organization have uniform and consistently enforced security policies?

If you answered no to any of these questions, then you need to incorporate controls that will ensure that users are adequately trained, monitored for policy compliance, and that there is fair and disciplined approach to enforcement of policy violations. This is not a trivial task, but it is a necessary one.

Security practices and protocols must be easy to use and must integrate transparently with your mission critical business processes. End users must be properly trained so they clearly understand the administrative, technical, and physical security policies and controls they are required to follow. If the security practices and protocols are too complicated or too disruptive to job performance, employees are likely to ignore them or find workarounds to avoid them. Regardless, it is all too easy to transpose data from its judicious use and purpose, to one of misuse and impropriety.

The following diagram depicts the variety of ways confidential information can be transformed.



Source: Enterprise Strategy Group, 2008

According to a 2009 study conducted by the Association of Certified Fraud Examiners, more employees are engaging in fraudulent activities due to deep cuts in salaries, staff, bonuses, and the fear of being tagged in the next wave of layoffs. In short, employees are stealing your information and using it to land their next job. Human Resources security and 'need-to-know' access are an integral part of a formidable solution. It is unfortunate, however, as reported by Gartner, that 84% of all security breaches come from an insider.

In 2008, the average cost of data breach was reported at \$6.65 million, based on the Fourth Annual U.S. Cost of a Data Breach Study conducted by PGP Corporation and Ponemon Institute. The US Chamber of Commerce, conversely, estimates intellectual property loss, at \$250 billion per year. Furthermore, a recent study conducted by SC Magazine found that more than 90% of a company's intellectual property is in digital format. The Internet, email, portable storage and mobile devices have increased the flow of information and subsequently created new threats to the security of intellectual property.

#### **Why are data breaches becoming so pervasive?**

*“It is easy to blame this dubious growth on mainstream security issues like software vulnerabilities, the explosion of malicious code, organized cybercrime or social engineering. These factors contribute to the problem but ESG believes that they ignore current data creation, distribution, and usage patterns.”*

The Enterprise Strategy Group, 2008

## **Getting Data Protection Right**

No company is immune from insider fraud, malicious leaks of inside information to the media, trade secret theft and economic espionage, along with a host of other internal and external attack methodologies, but the negative impact of such attacks is growing significantly. Moreover, information security has become a colossal business risk and enterprises are searching for smarter ways to deal with it.

The main goal of enterprise security is to protect the organization's ability to function through its assets: personnel and human capital; data and information; hardware; software; and technologies—all part of the equation. But pressures are mounting for security implementations to do much more. Not only must security be nimble and quick to comprehend and mitigate security incidents before they occur, security investment dollars must improve operational efficiency through end user transparency, seamless integration for enhanced workflows—all this while at the same time reducing costs. This may seem untenable at first take, but it is attainable through a security implementation featuring counterintelligence security protocols and enterprise rights management technologies.

## **Strengthening Security Management with the Counterintelligence Model**

Keeping an eye on unstructured data and critical information assets is no easy task when you are not sure what they are, where they are, and who has access to them. The fact of the matter is that critical information is walking out the door every day undetected.

In government, counterintelligence is the function of identifying and stopping foreign spies and terrorists. Every terrorist attack, for example, is preceded by an intelligence operation in which attackers gather information that is then used to develop and execute their plan. Agents must get inside the intelligence stream to stop the attack before it occurs. The same is true of commercial enterprises. Security professionals must get inside the activity stream to identify and close gaps that put the enterprise at risk.

A counterintelligence officer or group collaborates with security stakeholders across the enterprise yet operates with autonomy to provide independent oversight and segregation of duties in security management. Its purpose is to identify internal and external threats to mission critical assets and

find answers to challenging questions such as:

- What assets are being targeted for theft or misappropriation?
- Who would benefit from having access to them?
- How are the assets being targeted?
- Who are the high-value human assets within the chain-of-trust that have access to them?
- Are they being targeted as an inside channel for access to the assets?
- How vulnerable are the targets to compromise and exploitation?

The counterintelligence model works to protect mission critical information assets across the enterprise and throughout the lifecycle. The formulation of a risk treatment strategy is derived from an assessment and comprehensive analysis of policies, procedures, and work practices within each of the following seven categories:

- **Human Resources** – to understand how data, information, and content is created, shared, and managed across the chain-of-trust
- **Organization** – to define the degree of cross organizational collaboration among stakeholders for accountability
- **Assets** – to determine what needs protection and how the information is inventoried, classified, and managed
- **Process** – to identify policies that govern the creation, use, distribution, archiving, and destruction of unstructured data and information assets
- **Technology** – to determine the effectiveness of security tools, technologies, and solutions
- **Physical** – to identify physical controls and potential vulnerabilities impacting security
- **Performance** – to assess the capacity to monitor, audit and improve security for operational efficiency and cost savings

One of the reasons data leakage is occurring with alarming frequency is not because organizations do not have security policies and procedures in place, but because they fail to adequately train their employees, monitor their actions for policy compliance, and enforce policies when they are violated. Counterintelligence takes a lead role in assuring that security is executed according to plan. Among other tasks, it develops specialized training as required for persons with access to sensitive assets, monitors operations for compliance, and assures that enforcement practices are fair and consistent. A good defense is a strong offense.

## The Emergence of Enterprise Rights Management

In response to the need to secure unstructured data, information, and content, two predominant technology platforms have emerged: Data Loss Prevention (DLP) and Enterprise Rights Management (ERM). DLP solutions are reactive in nature and presume that critical data and information assets within the enterprise environment are 'unknown'. Parameters must then be created to identify such information in order to enforce security policies governing its usage. ERM solutions, on the other hand, are proactive in nature and presume that critical information assets

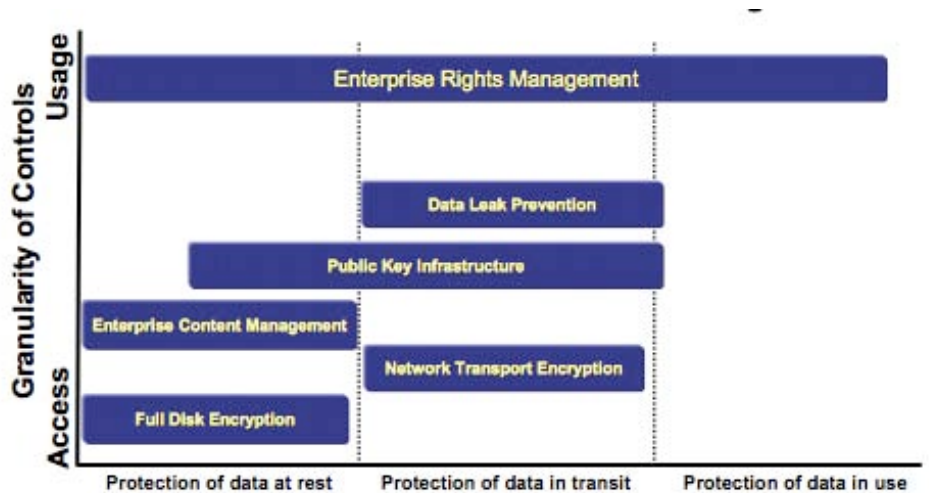
are 'known'. Security policies determining who may access them and what actions they may apply to them are easily enabled and transparently enforced.

This ERM solution provides three types of security: protection, control, and audit. Below is a description of each:

1. Protecting the document – the document and its content are encrypted while at rest, in-transit, and while in use. In addition, data on the clipboard is protected at all times.
2. Controlling access to the data – enterprise/business units define controls regarding who can access unstructured data and what actions they can apply to it.
3. Auditing the use of protected unstructured documents—audit capabilities track user attempts to access unstructured data and reports on what they have done after accessing it.

Business productivity relies on access to mission critical information, and today's knowledge workers demand around the clock access to company data seven days a week. Better access and collaboration platforms equal better business results. Complicating this is the exponential increase in mobile devices, virtual workstations, and the general portability of information. This portability of information can invoke fear and apprehension causing enterprises to downshift into a 'lock-down' mode to avert security risk. This would be unfortunate—and indeed unnecessary. Forward-thinking enterprises are looking for smarter ways to accomplish both portability and security. They want intelligent management strategies to revamp how data, information, and content is created, distributed, and used. Consequently, there has been a growing interest in solutions that offer more granular control of information and its use by multiple users, in diverse business processes, and in distributed work environments worldwide.

The following diagram shows the persistent control of access and usage of information assets.



Source: Enterprise Strategy Group, 2008

## Why Enterprise Rights Management?

The bottom line in today's world is that security must enable the sharing of information in collaborative and highly distributed work environments, while at the same time securing it through

dynamic centralized management controls that persist beyond the firewall. This is a daunting task with a conventional approach, as security has a lot to do with technology and everything to do with people. The key is fusing them together into one.

Enterprise rights management is emerging as a preferred solution among best of class organizations in order to meet security and compliance objectives, while at the same time complementing their existing repertoire of Data Loss Prevention capabilities. None of the legacy security solutions have been able to address the ‘unstructured data’ security dilemma like enterprise rights management, according to CIO/Insight.

The solution enforces centrally defined data access and information usage policies that persistently protect critical content. This enables you to promote both a collaborative environment and secure data content, without changing the way the users work. The assigned policies, combining encryption and other controls, regulate what actions a user may apply to the content, as well as follow it everywhere it goes. Furthermore, the solution enables the content to communicate detailed audit trails back to the policy server for review and oversight.

Enterprise rights management solutions close a huge gap and vulnerability by providing security to data in use. Until now, there has been no way to secure it. Security can now be viewed as a business enabler, where sharing and securing co-exist. According to Gartner, it will not be long before enterprise rights management will be adopted as a default solution—another mega-trend in security evolution. Among the benefits of this solution are:

1. The use of encryption to protect data at rest, in back-end systems, in transit on the network, and while in use at endpoint systems
2. The enablement of data sharing and data protection between internal users and the chain-of-trust
3. The granular control over the actions that may be applied to data (e.g., read-only, print, cut-and-paste, edit, save etc.)
4. The enablement to proactively prescribe via policies what actions a user may apply, as opposed to what they may not.
5. The ability to provide persistent protection, even when network access is unavailable
4. Access to detailed visibility into the enterprise’s data flow (e.g., who accessed it, how they accessed it, and how it was used)
5. The power to enable dynamic role-based policy creation for integration with identity and access management systems

## **How does Enterprise Rights Management Work?**

When a file is protected, policy keys are used to encrypt it. When the file is accessed, the local agent authenticates the user then decrypts the file, but blocks actions that are not assigned to that user in the policy that is protecting the file. Documents remain protected on both sides of a firewall and can only be accessed by authorized users. Permissions can be revoked or modified without redistributing protected files, and user actions are logged and stored for auditing, if necessary.

That being said, not all enterprise rights management solutions are the same. Having a secure container for information is not enough. Enterprises must protect the information itself so that it can remain secure while in use. Sitrof favors ERM solutions that provide ‘policy propagation’. This

means that when an authorized user accesses a file, ordinary functions like copy, paste, save as, and PDF conversion remain available; however, any new information or documents created retain the original security policies and settings. More simply put, policy protected content can be copied and pasted from a protected document into an unprotected document and remain securely protected. This protection can even transcend different applications. Security in action—where the rubber meets the road!

## **Bringing it All Together for Security, Compliance, Operational Efficiency**

Over the years, Sitrof has collaborated on, integrated, and deployed hundreds of complex enterprise content management systems. As a result of this vast experience we have developed the concept of intelligent unstructured data management (iUDM), which is comprised of products and services that enable organizations to view their unstructured data in an entirely new way. Enterprises can glean business intelligence, extract unrealized value, and bring order and security to an otherwise vast sea of unstructured chaos and risk.

Our proven approach in iUDM is defined in each of the following service domains:

### **1. Discover**

Discovery is an important first step in security management because data and information assets cannot be protected if they have not been identified. With the iUDM foundation in place, your metadata and content are crawled, creating an unstructured data topology map delivering unprecedented visibility across the most critical unstructured data sources. This capability was built in response to client demands for a better way of identifying unstructured data assets.

### **2. Assess**

Once assets are identified, an assessment must be done to determine risk. Sitrof conducts a comprehensive assessment of unstructured data management practices to determine the current state of security risk. The assessment combines personnel interviews, content and data topology mapping analysis, and a questionnaire methodology for an in-depth analysis under the following domains—human resources, organization, assets, processes, technologies, physical, and performance.

### **3. Define**

Not all unstructured data is worth protecting. But what is worth protecting must be properly identified, classified, and labeled to reflect the designated security handling requirements. This domain focuses on identifying critical information assets, business processes and applications that are most critical to competitive advantage, business innovation, profitability, corporate governance and regulatory compliance. These key processes or applications are defined according to: application type, data types and uses, user-participants of the application data, and infrastructure dependencies that may exist in implementing a technology based solution. The results of this service domain are captured in an application process map and incorporated into the documented security plan.

### **4. Plan**

Security cannot be effective without a well thought out plan. Combining the results of the preceding service domains of Discover, Assess, and Define, Sitrof 'Brings it All Together' into a comprehensive security management plan including persistent protection, control, and audit capabilities through a dynamic ERM technology platform.

The plan is a roadmap for implementation and consists of the following components:

- Management Plan - including charter and schedule
- Vision and Deployment Strategy - created for unstructured data security management including the Enterprise Rights Management technology platform and infrastructure
- Current State Risk Assessment Review - consisting of critical department users/system usage; technology infrastructure shortcomings; and software deficiencies
- One to Three Year Implementation Roadmap - outlining a phased deployment approach which maximizes risk protection

## 5. Implement

Sitrof offers a full service deployment team that will take the information gathered during the previous phases and install and configure a solution that satisfies the client's objectives. Sitrof technicians will document relevant installation and configuration settings made in a Configuration Specification. Sitrof personnel will also conduct training sessions to ensure that all users understand how to use the solution.

## 6. Improve

Security is a process that requires continuous review, analysis, and improvement. In this service domain, Sitrof collaborates with your organization to perform logical next steps to extend your security strategy for enterprise-wide deployment, operational enhancements, and integration of security dashboard tools for centralized control and visibility. The Sitrof team captures opportunities from initial engagement through project completion, providing your team with a documented roadmap outlining the ideal steps necessary to accomplish future state security goals and objectives.

## 7. Advise

Security is complicated. The implications of change through business innovation and threat innovation are far reaching and require expertise at all levels—both inside and outside the organization. In this service domain, Sitrof assumes the role of trusted advisor and partner to augment your security team's mission. This additional support is accomplished through email alerts, advisories, quarterly newsletters, Sitrof Security Summit Events focusing on the insider threats, counterespionage, and innovative applications of enterprise rights management that support counterintelligence goals and objectives.

## Conclusion

In today's distributed business models and ever expanding chain-of-trust, there are no guarantees when it comes to security. But one thing is for sure—you cannot afford to get data protection wrong. Good security is ubiquitous and occurs long before the end-user is granted access to critical information assets. By combining the *counterintelligence security model* with *enterprise rights managements*, organizations can raise the bar on security management to unparalleled heights.

Rather than protecting the information 'container' alone, it is now possible to embed security into the information itself. When this occurs, your organization's prescribed information access and use privileges can be centrally managed, monitored, and enforced when the data is at rest, in motion, or in use. Enterprise Rights Management changes the security paradigm. Senior executives can roll the

dice and take a gamble that point solutions will be sufficient, or they can adopt a holistic approach and get it right—Rights Managed that is.

## About Sitrof Technologies

Sitrof Technologies, Incorporated is a professional services organization with specialized expertise in information systems and solutions that guide organizations toward making strategic decisions, identifying risks and maximizing their data protection. Through Sitrof's years of experience in enterprise content management and espionage prevention, we can help you implement counterintelligence methodologies into your security management program, apply iUDM best practices, and deploy dynamic ERM technologies that offer visibility, control, and accountability.

---

**David F. Drab, CISSP, Director of Security, Sitrof Technologies, Inc.**—An accomplished information security professional with FBI investigative and enterprise security experience. He is a published writer and frequent public speaker on global security threat issues and risk mitigation best practices. He is a Certified Information System Security Professional (CISSP).

Mr. Drab is also a Senior Partner of The Insider Threat Mitigation Group, LLC. The organization applies the expertise of FBI/CIA field operatives to protect human resources and information assets in commercial enterprises worldwide. Prior to joining Sitrof, Dave was a Consultant and Security Thought Leader at Xerox Corporation where he and his team developed solutions to secure data, documents, and content across complex workflows for Fortune 500 enterprises. He is a 27-year veteran of the FBI with extensive field experience in organized crime, terrorism, and economic espionage. He successfully investigated the first case indicted under the Economic Espionage Act of 1996 in which foreign government sponsorship was charged. He is an Executive Advisory Board member for the U.S. based Homeland Defense Television (HDTV) network.



*“Perhaps at no other time in history has information been more valuable and vulnerable at the same time. For this reason, the sophisticated methods and techniques of espionage are widely used to gain access and acquire all types of information, not just trade secrets for competitive and economic gain. Consequently, enterprises must do some things better and other things smarter. First, get a better grip on unstructured data: what it is; where it is; and who has access to it. Second, add the counterintelligence model to manage security beyond technology. Lastly, implement an enterprise rights management technology platform for persistent security of data wherever it is. The result is a security implementation and culture that is more preventive, preemptive, and predictive.”*