Preventing Document Leaks

TITUS White Paper
At Titus we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.

For further information, contact us at (613) 820-5111 or email us at info@titus.com
# Table of Contents

1.0 | Introduction ................................................................................................................................. 4  
2.0 | The Costs of Information Leaks ................................................................................................... 5  
3.0 | Securing Information from Widespread Distribution ................................................................. 7  
4.0 | Titus Solutions ............................................................................................................................... 8  
   4.1 | Titus Message Classification and Document Classification ...................................................... 8  
   4.2 | Titus Metadata Security for SharePoint ...................................................................................... 8  
   4.3 | Titus Solution Example ................................................................................................................ 9  
5.0 Conclusion .................................................................................................................................. 11
1.0 | Introduction

Documents, records and information are important assets for any organization: military, government or commercial enterprise. Organizational documents can often contain tactical plans and military intelligence, confidential policy or financial data, intellectual property, personal information and a host of other sensitive topics. There is a general understanding by people working with these types of information that some form of security is required to protect such important data. Many of these organizations have put in place sound IT infrastructure to protect sensitive documents, ranging from encryption mechanisms to private secure networks.

However, the need for immediate access to information, as well as the need to share information internally or externally, has created an environment where sensitive or confidential documents may be accessible to a large number of individuals. Widespread access to such information can pose serious risks as there is a greater chance of an individual exposing the information. Even classified information stored on secure and physically separate networks is subject to inadvertent or malicious disclosure.

In addition to IT security infrastructure and physical security, organizations require policies which restrict access to confidential information to only those individuals that truly require access. The challenge arises in applying such policies quickly and consistently to the vast amount of confidential documents and information being created every day.
2.0 | The Costs of Information Leaks

There have been many examples in the past few years where document leaks or leaks of confidential information have lead to embarrassing or even dangerous results. We can examine these leaks to learn how to structure proper information handling policies, as well as the costs of such leaks.

In the fall of 2006, several documents were leaked from the internet company Yahoo! relating to a possible acquisition of Facebook. The acquisition described by the set of documents was called “Project Fraternity” and was published by several internet technology news sites (e.g. TechCrunch). They include strategies, valuation and acquisition pricing as well as details of negotiations. The true cost of this leak is difficult to determine, but the early exposure of acquisition related details can often put acquisitions in jeopardy.

In July 2009, 310 sensitive executive level documents were leaked from the social networking company Twitter. These documents included financial projections, personal phone logs, security pass codes and executive meeting notes with highly confidential information. The leak was caused by an individual external to Twitter compromising the personal accounts of a small number of lower level Twitter employees, thereby gaining access to large amounts of high-level sensitive documents and data. The leak of these documents resulted in embarrassment for the company and for some individual Twitter employees. In addition, it exposed high-level strategic and financial information to the company’s competitors.

In October 2009, a 2,400 page document called the Joint Services Protocol 440 was leaked from the British Ministry of Defence and posted to the internet. This document contained specific instructions for the intelligence community on how to avoid leaks in information flow due to hackers, journalists and foreign spies. The leak drew major worldwide media coverage and, in addition to possibly compromising intelligence strategies, caused serious political embarrassment for the governments involved.

In July 2010, there was a massive document leak of over 91,000 records covering the U.S. led war in Afghanistan from 2004 to 2010. This set of records is referred to as the Afghan War Diary and a subset of approximately 75,000 records was made available to the public on the WikiLeaks web site. The reports, written by soldiers and intelligence officers, describe lethal military actions involving the United States military, but they also include intelligence information, reports of meetings with political figures, and other sensitive details. Although these reports were stored on the U.S. secret secure network named SIPRNet, which is physically separated from all other networks, a large number of people had clearance to access them. As a result, these reports were extracted from the system’s repository, reviewed by an external team of individuals who did not have appropriate security clearance and were made public to a worldwide audience. The associated costs with these leaks are quite varied and serious – they range from political embarrassment, to compromising the military mission, to endangering the lives of military personnel and associated support/aid staff.

Although the scale and costs of these leaks varies, in all cases, the information leaks can be attributed in part to the widespread distribution of confidential information. To illustrate how widespread this access is currently in the United States of America there are approximately 854,000 people, more people than the population of San Francisco, that have top secret security clearance (source: Washington Post Investigation: Top Secret America, July 19, 2010 - http://projects.washingtonpost.com/top-secret-
This means that a large part of the population has access to America’s most closely guarded secrets. With such a large group of individuals having access to large amounts of classified information, the likelihood and risk of leaks occurring is very high. Another way to look at this challenge is that even if people have Top Secret security clearance for certain special projects, it does not mean that they should necessarily have access to all the information on the top secret network. Exposing sensitive information to large groups of people dramatically increases the risk of leaks.
3.0 | Securing Information from Widespread Distribution

The most important step in securing information is to understand what information is truly sensitive and what information can be freely shared. Information classification can be used to accomplish this objective. Securing sensitive information in an environment that is widely accessed requires both the establishment of strong classification and handling policies, and the consistent and automatic application of those classifications and policies by both individuals and systems. In order to efficiently control the distribution of large amounts of sensitive information, classifications must be applied to documents and data. But classification alone is not enough. Once classified, security permissions to access that information must be automatically set based on those classifications.

This results in an easily enforceable classification-based security strategy for controlling access to sensitive information. The outcome will be to reduce and better control the number of individuals that can access sensitive information, and thereby reduce the risk of inadvertent or unauthorized/malicious disclosure.

The first step in this strategy is to classify documents and information with caveats. Traditional information marking is useful to communicate classification, as it provides a visual indicator to users on how to handle the information (e.g. first or last line of email, headers, footers or watermarks in documents). Unfortunately markings in themselves do not provide any additional security, in the form of controlling access to or the distribution of information. However, information classification which embeds metadata into a classified email or document does provide intelligence which can automatically result in additional security, such as controlling permissions, applying encryption, and invoking enterprise rights management.

The second step is to automatically assign security permissions to the documents or information based on its classification metadata, with the purpose of controlling access. This will allow consistent and efficient application of security policies around the handling of sensitive information. This will also serve to automatically control and limit the audience that can access a particular document or piece of data. Even in situations with large amounts of confidential data being continually generated, the automatic process ensures that security policies are always enforced, and enforced in a consistent manner.

Figure 1. Controlling the audience that access confidential documents through the use of classification and metadata based security greatly reduces the risk of accidental or intentional disclosure.
4.0 | Titus Solutions

Titus is uniquely positioned to meet the requirements necessary to prevent information leaks. As the leading provider of user-based email and document classification solutions, as well as metadata based security solutions for Microsoft SharePoint, Titus offers a complete information marking and security solution for the Microsoft Office platform.

Titus products include:

- **Message Classification™** for the marking of emails in Microsoft Outlook®, Outlook Web Access®, and mobile devices
- **Document Classification™** for the marking of Microsoft Office Word®, PowerPoint®, and Excel® documents
- **Metadata security** solutions for Microsoft SharePoint Server®
- **File server marking** solutions for Microsoft Windows Server 2008 File Classification Infrastructure® (FCI).

4.1 | Titus Message Classification and Document Classification

Titus Message Classification and Document Classification are user-based information classification tools that embed classification metadata in emails and documents, in addition to applying visual labels and markings. These tools can also trigger additional levels of protection based on the classification, such as the automatic application of Microsoft Active Directory Rights Management Services® (RMS) or S/MIME protection for email. With features like caveat support, signed trusted labels, guided classification for more complex classification processes, and customizable markings and metadata, Titus Message Classification and Document Classification products provide a full featured solution to government, military and commercial organizations which help them enforce their classification policies and prevent inadvertent disclosure of information.

4.2 | Titus Metadata Security for SharePoint

Titus Metadata Security for SharePoint is a security solution for Microsoft SharePoint Server that automatically applies security permissions to files based on the file’s metadata. Automatically applying permissions based on classifications and caveats results in a controlled and more restricted audience being able to access documents, thereby lowering the risk of disclosure.
4.3 | Titus Solution Example

Often organizations will have support staff access senior executive planning documents as part of their daily work. However, they may still wish to keep very sensitive documents, such as compensation plans, restricted to being accessible only by the senior management team. Titus Document Classification allow the originators of these documents to classify them as ‘Confidential’ or ‘Confidential – Restricted’ (figures 2 and 3) and store that with the document’s metadata.

![Figure 2. Sensitive documents such as compensation plans can be classified through Titus Document Classification to mark them with the classification labels of Confidential and Restricted, to highlight their sensitive nature.](image)

![Figure 3. In addition to visual markings being applied, metadata relating to selected classifications is stored with the documents, enabling server solutions to automatically set access permissions on those sensitive documents based on their classification.](image)
Based on the document’s metadata, Titus Metadata Security for SharePoint will then automatically set permissions on those documents within SharePoint so that a CEO will view and access all documents (Figure 4) but an Executive Assistant for example may only access a subset (Figure 5).

**Figure 4.** CEO’s view of the SharePoint document library: Fiscal 2011. All documents marked Confidential or Confidential-Restricted are available for the CEO to view and access.

**Figure 5.** Executive Assistant’s view of the SharePoint document library: Fiscal 2011. Only documents marked Confidential, and not Confidential-Restricted, are available to the Executive Assistant.
5.0 Conclusion

Organizations require policies which restrict access to confidential information to only those individuals that truly require access. Applying such policies quickly and consistently to the vast amount of confidential documents and information being created every day can be very challenging.

The most important step in securing information is to understand what information is truly sensitive and what information can be freely shared. Information classification can be used to accomplish this objective. But classification is not enough. Once classified, security permissions to access that information must be automatically set based on those classifications.

An easily enforceable classification-based security strategy for controlling access to sensitive information can reduce and better control the number of individuals that can access sensitive information, and thereby reduce the risk of inadvertent or unauthorized/malicious disclosure.


To learn how Titus can help your organization promote information sharing, please visit www.titus.com.

Titus
343 Preston Street, Suite 800
Call us: (613) 820-5111 ext.127
Toll Free 1-866-530-5111
or email us: info@titus.com