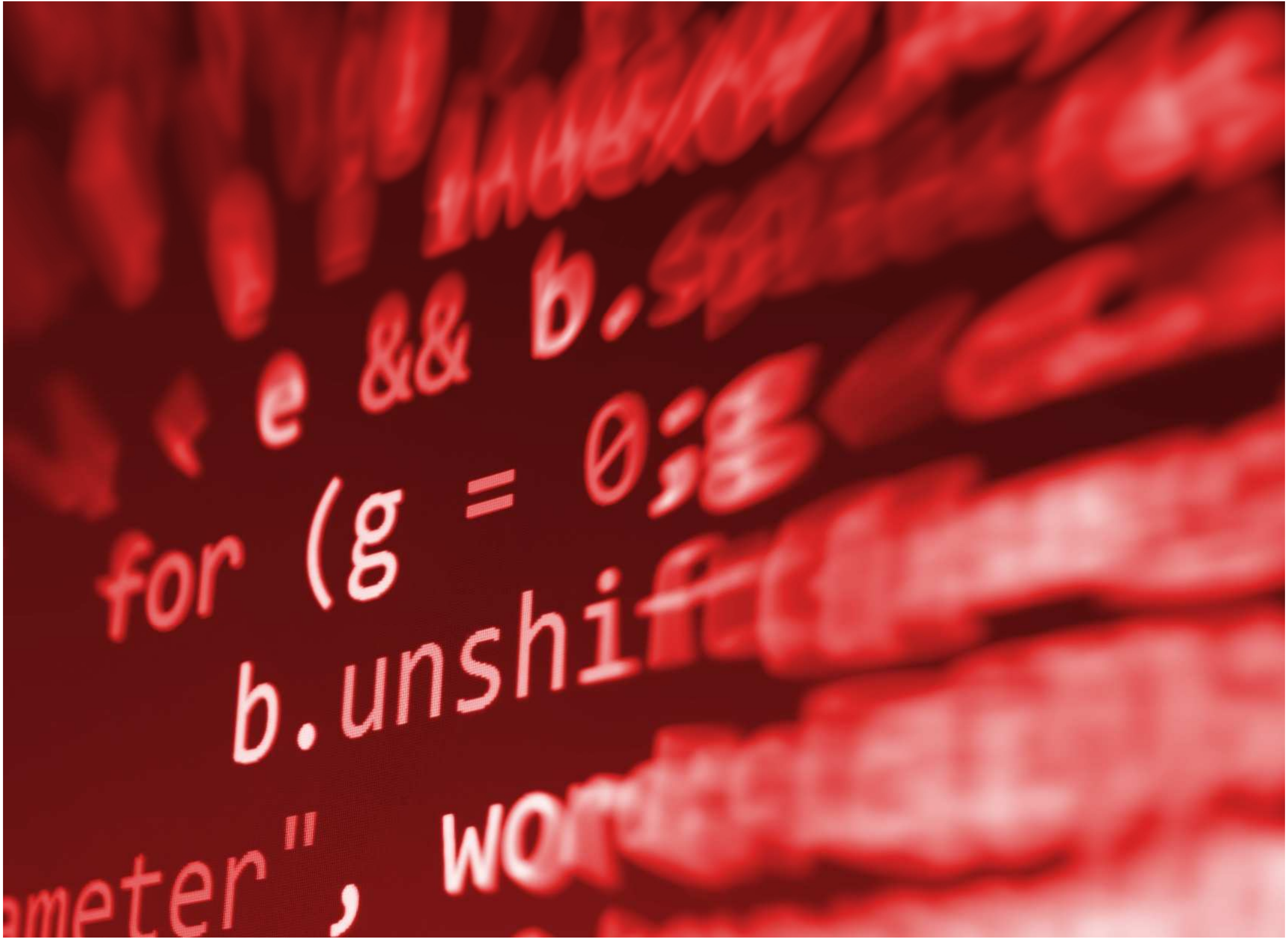

Sacrificing Security for Mobility?

Understanding Metadata for Today's Mobile Professional

Professional Guide: 5 Tenants of Metadata and Metadata Cleaning Solutions. Securely Optimize Work Performance with the Freedom of Mobility.

A Litéra Corporation White Paper | November 2015

Abstract

While many professionals continue to work from the office, an increasing number are choosing to work from home, using their mobile device, tablet, and laptop to operate. The robust processing applications once exclusive to office desktops are now supported by most operating system's in most cell phones.

Mobility for professionals is proven to build symbiotic relationships between employee and employer. However, the benefits of mobility are not worth a tarnished reputation. Fortunately, a concrete understanding of metadata and metadata cleaning solutions give people the mobility they want with the security they need.

Metadata control is an ongoing battle for professionals' and has been for over 40 years. This special report includes a solution to the frequent problems metadata creates for professionals.

Professional's solution to understand and control metadata:

1. Comprehensive understanding of metadata's fundamental tenants - definition, source, type, identification and locating.
2. Find a robust metadata cleaning solution; providing both a proactive and reactionary solution to unintentional metadata exposure.
3. Know what causes metadata related leaks and/or breaches. In addition to dispelling the common misconception that metadata leaks and/or breaches are always the work of hackers.

TABLE OF CONTENTS

The Problem with Metadata

In today's business environment professionals are afforded the luxury of a flexible work environment. There are dozens of mobile devices that support the same robust desktop applications being used in the office. Mobility is a gift that gives professional's the freedom to work anywhere on almost any mobile device, tablet, or laptop. The problem with mobility is metadata.

Metadata is complex and difficult to control; its presence is elusive, capable of living in ostensibly confidential documents forever. While professionals' today are increasingly afforded the freedom of mobility, conducting business outside of the office sets a dangerous precedent for professionals.

Leaving unidentified metadata in a company document significantly increases the chance of experiencing a data leak or breach. This should be especially concerning for mobile professionals. Whether at home or in the office data leaks are far more likely to be caused by human error than hacking. Consequently, mobile professionals' are more susceptible to a data leak or breach than employees working from the office. As such, professionals' need a comprehensive understanding of metadata in addition to effectively operating a metadata cleaning solution.

This special report explains what, where, and how metadata is generated in addition to the latest strategies being used to enhance mobility, understand, control, and manage metadata.

Metadata Explained

What Professionals' Must Know About Metadata in 2016

Metadata Defined
The most common phrase used to describe Metadata is, 'data about data.' While 'data about data' does not incorrectly describe metadata, it's vastly incomplete. A more precise definition of metadata is, "structured information that describes, explains, location, or otherwise makes it easier to retrieve, use, or manage an information resource**^1**."

Sources: Application, Desktop, and System Metadata
Metadata is initially broken down by document and application metadata. Document metadata includes tracked changes, hyperlinks, hidden text, comments, date, time in addition to 70 or so more details describing a document's history**^2.** Application metadata is information about your software applications and the third-party tool used to generate, convert and format a document.**^2**

System metadata can be made up of application and document metadata. Your system metadata displays the operating system, server and printer name associated with that document. The following scenario illustrates a common metadata dilemma professionals' experience.

You recently purchased a laptop and are transferring data from one system to another. When your documents are downloaded to a new system they are time stamped.^3 The time stamp provided by system metadata does not always accurately reflect the lifespan of a document; it only reflects when the document and system interacted. **Solution** - If you're searching for accurate metadata but have completed a system transfer, look at your existing document and application metadata for more accurate information.

Types of Metadata
Descriptive Metadata
The phrase descriptive metadata, is self-explanatory and more easily understood keeping that in mind. Descriptive metadata reveals or describes a resource that a content owner can use for discovery or identification purposes. Descriptive metadata include the following document components: title, abstract, author, and keywords. This is the metadata you're likely familiar with.

Structural Metadata
Structural metadata is the least complex and most helpful of your metadata bulk. A good way to remember structural metadata is to think of the page numbers in a paperback book. Structural metadata is the digital equivalent of printed page numbers. "Structural metadata is commonly used to facilitate express the

intellectual boundaries of complex objects by facilitating the navigation and presentation of complex sequences."^5

Administrative Metadata

"Data that is necessary to manage and use information resources and that is typically external to informational content of resources"^6. Administrative metadata reveals the context necessary to understand how the metadata originated. For example, administrative metadata tells the user aspects of data creation, acquisition, rights management and disposition.^7 Administrative metadata encompasses several subsets of data. Rights management and preservation are two subsets of administrative md that professionals often claim are individual types of Metadata.

Rights Management

Rights management metadata is a sub-category of administrative data. It deals primarily with intellectual property rights. With intellectual property issues clogging dockets for at least a decade, rights management metadata has become central in privacy debates among legal scholars and professionals alike.^8

Preservation

Preservation metadata contains information required to archive and preserve a resource; much of today's cybercrime can be traced to preservation metadata. Metadata is key to ensure resources will survive and continue to be accessible in the future, but the fragile nature of digital information has organizations worldwide aggressively searching for a solution that effectively protects preservation metadata.

Metadata Purpose

An incorrect but popular belief is that software maliciously embeds harmful metadata into documents for easy disclose of confidential information. While metadata type and bulk size vary for each user, its purpose and function are rooted in utilitarian ideologies. The overarching purpose of metadata is to make our lives easier. For example, document metadata is a great tool for tracing misplaced and/or stolen content provided you're a legitimate document owner. It's also a great tool for document owners to revise, organize and access electronically-created files. [Metadata: The Ghosts Haunting e-Documents].

PURPOSE	FUNCTION
Resource Discovery	A. Pinpoint document location B. Identify resource with relevant criteria
Organize eResources	A. Bunch like-resources B. Locate unfamiliar resources

Digital identification	A. Differentiate one object from another B. Combine metadata to identify data
Archive and Preserve Interpolarity	A. Sustain resource access B. Guarantee future access

Metadata Cleaning Solution: Protect Your Organization's Reputation!

Every time you edit a document you create metadata. Metadata is the silent companion that travels with every document and can kill your reputation or accidentally leak valuable information to a supplier, customer or competitor. Imagine if others knew when you had edited a document, who had made comments and what those comments were. Or, if pricing could be reverse engineered because a spreadsheet went out with formulas intact.

There are two primary methods to clean metadata manually catalogue or apply a metadata cleaning solution. The former approach is unnecessarily time-consuming and leaves organizations open to a potentially grave human error. Because metadata is often unrecognizable, the manual approach heightens your risk of unintentional leaking sensitive information. As such, professionals working remotely or from the office need a metadata cleaning solution.

According a survey done by Litera Corporation in 2012, "96% of business professionals polled are using mobile devices to store, access and send sensitive material, and the majority are doing so without e-mail encryption or metadata removal, thus posing significant security risks to their organizations. Companies are beginning to recognize these risks and one third of the IT respondents say they now have server-based metadata scrubbing tools."

This survey also found that:

A. 96 % of respondents said they use their devices to access business e-mail messages every day.

B. 89 % store business documents on their mobile devices

C. 86 % forward e-mail with document attachments at least once a month (30 percent said they do so multiple times each working day)

D. 34 % have access to their organization's document management system from their mobile device

With last year's number of data breaches affecting nearly 50 percent of companies' worldwide^8, a 10 percent increase from 2013, its imperative organizations have a metadata cleaning solution in 2016. Metadata is a digital paper trail and should be treated that way. A paper trail can lead anywhere or primed to mean anything; a metadata cleaning solution keeps your metadata bulk secure and reputation protected.

According to the ALCTS, "In the current discovery environment, it is difficult to measure what is not found and extremely difficult to quantify the impact and cost of poor, incomplete, or missing metadata on business and collection analysis decisions that ultimately affect consumers." Think about that, not only can metadata become part of the public domain quickly but the metadata owner can't quantify the consequences until whoever stole the data is caught or stop using the metadata.

Companies' without a metadata cleaning solution are more frequently presented with the task of dealing with managing a data breach. Manually monitoring, storing and cleaning metadata is not only inefficient and ineffective, but has a far lower success rate in preventing a metadata leak/breach than a company that uses a metadata cleaning solution. If your company has confidential documents, it's imperative to have a metadata cleaning solution

Understanding Metadata: Data Leak and Data Breach

Professionals must understand how to control metadata and the risk it poses when working from in the office or from home. A common misconception about metadata causing a data leak or breach is that someone hacked the system. Hackers are far from the most likely cause of a metadata leak and not the most probable candidate for a breach either; the leading cause of both these scenarios is human error.

USA TODAY's Elizabeth Weise recently reported, "While shadowy hackers in Eastern Europe often get the blame for these attacks, more than 80% of the breaches that Bruemmer's Experian Data Breach Resolution Group works with had a root cause in employee negligence . . ."

According to Privacy Rights Clearinghouse, here are the most frequent causes of both data breaches and leaks:

Metadata and Mobility - Data Leak 4 Times More Likely Result of an Internal, Employee Human Error than Cybercrime:

A. Non-compliance with corporate policy
B. Neglect to communicate using a secure network
C. Storing content on a secure server
D. Failure to control, monitor or clean metadata from company documents

Albeit a sad reality, cyber theft will leave an organization penniless and broken, left only with the scattered remains of a sullied reputation and an insignificant embedded image. If there is one takeaway from this special report it's this: Educate your employees on metadata. By conveying this information, professionals can use secure channel to create, control, collaborate, and securely share documents without the concern of experiencing a data leak or breach.

Key Takeaways

Definition
Metadata is a complex, highly-compartmentalized form of the modern day paper trail. The most effective tool for understanding metadata is a funnel. With a funnel analysis, broad definitions are examined initially followed by more pointed definitions and so on. This funnel analysis will provide reader's with a comprehensive understanding of metadata and its many intricacies'.

Source
Metadata is generated every time a keystroke is hit. The next step is to locate where the metadata was generated and from what source; besides your fingers tapping the keyboard. There are three categories of metadata: document, application, and system. System metadata can include both, one, or neither document and application metadata. (I understand it, but are you trying to write a tricky sentence?)

Types
Metadata identification is further synthesized by type. There are 5 types descriptive, structural, administrative, rights management, and preservation metadata. Traditionally rights management and preservation metadata are subsets of administrative metadata. Over the last decade rights management and preservation metadata are central topics in debates regarding cybersecurity, leading to their reclassification as independent metadata types.

Purpose
The purpose of metadata is to help people identify, extract, and edit digital content. Metadata is the digital equivalent of a paper trail, its purpose is allowing content owners to keep updated tabs on their documents. Metadata is a great tool for organizing and locating content, however illicit behavior has made metadata an immediate threat to any professional and their organization.

Protect Reputation
Metadata can be helpful or crippling, the outcome depends on content control. Organizations as well as Professionals need to understand how to clean metadata and bolster content control. Content control and mobility go hand-in-hand and

should be treated as such. Consumer reliance on mobility is a key factor when determining the best approach for keeping metadata under control.

Data Leakage – Stop Giving Hackers Credit!
Primarily human error. On scale of people affected, hacking typically higher because the intent, but generally speaking data leaks are 4x more likely to be caused internally – by employee error – than a hacker. Know the facts, if you don't know the past, you're bound to repeat it.

About Litéra – The Content Confidence® Company

Litéra's content solutions protect reputation, manage risk and increase productivity, providing the control and mobility you need. We help you get the job done securely, on any device, from anywhere.

Litéra's comprehensive productivity and risk management suite provides organizations with unsurpassed Content Confidence®. Patented document creation, collaboration, and control technologies streamline workflows and provide a new level of information security with governance at the document level, even outside the organization. These capabilities are now available in any location, on any device, in any environment with Litéra Anywhere™. This allows remote users simple access to the tools and content they always need to do their job, and facilitates cyber-secure and effective collaboration between disperse mobile users, teams and organizations. Learn more at www.litera.com

Litéra Solutions Are Tailored to Meet All Your Content Needs: Document Management - Multiple Document Version Management - Hidden Data Management - Email Management - Content Creation - Content Control - Control Collaboration - Approvals - The Cyber threat - The User Threat