The Risks in a Mobile World of Hidden Data in Documents

How Confidential Information Is Pouring Out of Your Business

Litéra Corp 2012
CONTENTS

Executive Summary ......................................................................................................................... 3

Document Metadata ......................................................................................................................... 4
  Document Metadata Leak Examples .............................................................................................. 4
  Emailing Documents ..................................................................................................................... 5

The Mobile Workforce and Email .................................................................................................. 6
  The Mobile Devices That They Use ............................................................................................... 6
  Email Access from Mobile Devices and Access Mechanisms ....................................................... 7
  Emails Sent from Mobile devices with Attachments ...................................................................... 7

Desktop Tools Will not Suffice ......................................................................................................... 7

Litéra’s Approach to Cleaning Hidden Information from Documents ............................................ 7

About Litéra .................................................................................................................................... 8

References ....................................................................................................................................... 9
Executive Summary

Hidden information in documents is often the source of the world’s most notorious scandals in business and government, causing leaks of closely held financial projections, R&D plans, client relationships, spy/whistle-blower identities and other highly sensitive information. Whether it be the history of tracked changes, comments, or other properties, this information can destroy an individual’s or an institution’s reputation and have a significant financial impact through fines such as for noncompliance, negative impact on stock value or damages from litigation. It can also have a lesser but more frequent impact on day-to-day content confidence in a business or government agency.

Information leaks can have many sources, but by far the biggest risk today is literally in the palm of your hand. The use of mobile devices in business has exploded in recent years, with a survey reporting that more than 40% of all emails are opened by a mobile device or access mechanisms such as webmail. A 2011 independent survey reported that 24% of all business emails sent each working day have files attached.

Most businesses and government agencies understand the risk of leaking sensitive information through metadata, and have had desktop document-scrubbing tools in place for years for external-facing users. What they did not predict was the meteoric rise of mobile devices and mobile access mechanisms, which, of course, bypass those desktop tools. Even with a desktop tool in place, this means that as many as 1 in 10 business emails could be leaking information via information hidden in documents.

This paper explains this specific risk area in more detail and explores some of the tools that mitigate the risk. The paper refers to results of a survey run by Litéra Corporation early in 2012 into “mobile device usage and document security” as well as surveys undertaken by other research groups.

It should be noted that the use of the term “document” refers to multiple file formats throughout this paper, including spreadsheets, presentations, photographs, faxes, PDFs and so on.

---

Document Metadata

Every electronic document has information contained in “metadata”. Some of the data is well known, such as author and date created. But what many people find surprising is that metadata can also contain all document revisions including insertions and deletions, tracked changes and comments added by reviewers, distribution of the document, total editing time, location of the stored file and more.

The information that metadata contains has its uses during the creation of the content of the document. When the document has been approved, or even if it is sent out prior to being finished, then this “hidden” information should be reviewed in the same way as the visible content to ensure that it does not contain anything that is sensitive or confidential. A lack of knowledge of what could be in the document’s metadata, a lack of process to ensure the metadata is reviewed, or even a lack of time that leads a busy document creator to simply accept all changes could well lead to disclosure of sensitive or confidential information.

Document metadata leak examples

The examples of agencies or businesses who have unintentionally disclosed information via document metadata are numerous. Some examples include:

- Metadata in a Merck document proved they had deliberately deleted relevant cardiovascular risk data on Vioxx prior to submitting it to the New England Journal of Medicine.4
- A dossier created by Tony Blair’s office and later presented to the UN by Colin Powell was used to support claims about a threat from Iraqi weapons of mass destruction that were used to justify war in February 2003. Metadata uncovered in the document later showed that much of the text was copied directly from a thesis published on the Internet by a U.S. researcher.5
- In 2006 Google let slip their financial projections via PowerPoint notes.6
- Shortly before release, photos of all 759 pages of Harry Potter, The Deathly Hallows were leaked. Fortunately for Scholastic, the photographer wasn’t aware that his Canon camera provided over 100 pieces of metadata!7

All businesses and government agencies must address the risk of unintentional disclosure of information via document metadata.

---

4 Chris Placitella, “Cos., Gov’t Seek to Keep Lid on Metadata”, 2006.
The reveal of a last-minute edit via tracked changes yielded the names of those thought to be involved in the 2005 assassination of Lebanon’s former Prime Minister, Rafik Hariri. New indictments continue in March 2012.8

No business or government agency is immune from the risk. All document format types can be a vehicle for unintentional disclosure of confidential or sensitive information.

<table>
<thead>
<tr>
<th>Jurisdiction/Source</th>
<th>Metadata Opinion/Ruling</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Bar Association Standing Committee on Ethics and Professional Responsibility12</td>
<td>SUSSIONED REMOVAL – Methods for eliminating metadata, including “scrubbing.” Are suggested to prevent sending opposing counsel a document that contains or might contain metadata [Formal Opinion 06-442], and to ensure compliance with Rule 1.6 regarding confidentiality of client information.</td>
</tr>
<tr>
<td>13 US State Bar Associations (AL, AZ, CO, FL, ME, MD, MN, NH, NY, PA, DC, VT and WV)12</td>
<td>REASONABLE CARE – 13 state bar associations ruled that attorneys must exercise “reasonable care” by taking steps to safeguard the confidentiality of client information in all communications sent by electronic means, including preventing inadvertent sharing of metadata with third parties.</td>
</tr>
<tr>
<td>Canadian Bar Association Ethics and Professional Issues Committee19</td>
<td>REASONABLE CARE – Lawyers have an ethical obligation, when transmitting documents electronically, to exercise reasonable care to ensure that clients’ confidential information is not disclosed in the metadata. [Rule IV, Commentary 4]</td>
</tr>
</tbody>
</table>

In the legal community, the risk is understood to be so high that 96% of medium-to-large-sized law firms have metadata removal tools in place1, and Bar Associations in the United States and other countries are ruling that metadata should be scrubbed to safeguard clients’ confidential information.

**Emailing Documents**

Email is still the primary mechanism by which a document is sent out from a business or agency. Overall, the average number of business emails sent out daily per user, according to the survey “Corporate Email 2011-2012” by the Radicati Group,2 has increased from 33 per day in 2010 to 41 per day in 2012.

Nearly a quarter of all emails sent in a business day have attachments.

Of most interest for this paper, this survey found that the proportion of emails that have attachments has also increased from 14% to 24% in 2011.

Although there are other document dissemination mechanisms that must also be included when looking at processes to mitigate the risk of information leakage from document metadata, email should be at the top of the list.

---

The Mobile Workforce and Email

The number of remote workers, whether at home, on the road or at customer sites, is predicted to continue increasing over the coming years.

A 17 country survey by Avanade\(^9\) found that 88% of executives feel their employees were using personal devices for business. Absolute Software\(^10\) found that 64% of IT managers thought it was too risky to let those devices be integrated into the business network but more than half allowed some form of access anyway. And Cisco\(^11\) found that although 48% of IT managers said they would not approve it, 57% said some employees use personal devices anyway, and the majority felt that BYOD was on the rise.

Applications and tools to support and encourage this increase in productivity are welcomed by all sizes of business. Equally, the additional risks from this type of working need to be addressed.

The Mobile Devices That They Use

In the 2012 Litéra survey\(^3\), BlackBerry, iPhone, and iPad were shown to be the most widely used (28.1%, 20.7%, and 24.4%, respectively). The survey also showed that the use of iPads will rise within this user base to 29% by the end of the year. Another survey\(^12\) of 1,600 business owners reported that 22% plan to purchase tablets for their users in 2012.

Since most of these devices are user-owned, companies are determining whether to purchase these devices proactively or use other methods to secure use. Also, with mobile phones, users forward documents but are unlikely to do significant document editing. Tablets allow much easier editing, which means more sophisticated tools are required, and a variety of security measures become much more critical.

Other surveys\(^13\) have focused on SmartPhones only, with many of them having Android and Apple’s iOS battling for top position, depending on the survey report and the RIM OS trailing. Although Litéra’s survey results show BlackBerry still having a strong position in the market, the results predict that usage of BlackBerry SmartPhones will decline over the coming year. Since those devices were considered the most secure from a data perspective, this may prompt additional data security measures.

---

\(^12\) ChangeWave Research, “Demand for New iPad Shakes Up Corporate Market”, 2012.
Email Access from Mobile Devices and Access Mechanisms

According to Litéra’s survey, 96% of all Smartphone and tablet users access business email from their devices and a third can access their companies’ central document store.

From a more general perspective, the number of emails that are accessed from mobile devices and mobile access mechanisms continues to increase every year. Averages taken from the results of other surveys indicate that about 40% of all business emails were accessed via a mobile device or mobile access mechanism in 2011.

Emails Sent From Mobile Devices with Attachments

According to the 2012 Litéra survey, 86% of mobile device users forward emails that have a document attached.

Additionally, 40% of users attach a document to an email that they send from their mobile at least once per month.

Fewer make actual edits (26% one or more times a month). It is very likely that this figure will be higher over the coming months and years with the projected increase in use of tablets.

Desktop Tools Will Not Suffice

With so many documents being sent outside of businesses every working day, the risk of leaking sensitive information hidden in these documents cannot be ignored. A desktop document metadata cleaning tool will not cover documents that are sent as email attachments from mobile devices and mobile access mechanisms.

Of the respondents to the Litéra survey who have a document metadata cleaning tool, less than a third have one that covers documents that are sent from mobile devices. Based on the statistics from the surveys covered in this paper, this means that these businesses are not cleaning 10% of the documents emailed despite having invested in document metadata removal.

Litéra’s Approach to Cleaning Hidden Information from Documents

Litéra has developed the only patented* document metadata cleaning solution that ensures that ALL documents attached to emails are automatically cleaned no matter how they are sent including via

---

86% of mobile device users forward emails that have a document attached

Businesses that have a desktop document metadata cleaning tool are not cleaning up to a fifth of the documents emailed.

14 Mark Brownlow, “Mobile Email Statistics and Use” 2011.
webmail, such as Microsoft® Outlook Web Access, and via SmartPhones or tablets.

Metadact® is Litéra’s server-based metadata cleaning solution that includes mechanisms for central policy management and a patented unified platform for mail gateways, which means that attachments of all Microsoft® Office files, PDFs, images, and ZIP files (from whichever source) are cleaned. Metadact® is intuitive for users or invisible as you desire. Metadact  also has on-demand cleaning and batch processing tools for internally stored documents.

Set up of Metadact  takes about three hours and requires no “babysitting” afterward. Simple reports on latency, message size, number of attachments, and so on, are available to help balance load and ensure optimal running of the servers.

Litéra’s outstanding support staff has created implementation kits containing user and installation guides, quick references, training videos, and sample e-mail communications, all available to help you breeze through every step of installation.

This user-friendly utility provides a mechanism to examine and clean documents before they are sent out. Metadact® integrates with multiple e-mail systems and Microsoft Exchange Servers.

Protect yourself and your company’s and your clients’ confidential information with Metadact®.

About Litéra
Litéra enhances professional productivity and risk reduction through a comprehensive suite of document creation, collaboration, comparison, control, and cleaning solutions. Litéra’s patented applications eliminate the need for tedious, error prone manual reviews and give you true Content Confidence® across complex spreadsheets, documents, presentations and PDFs.

For more information, visit [www.litera.com](http://www.litera.com)

Litéra, Metadact and Content Confidence are registered marks of Litéra Corp.
* Patents 7,895,276 & 8,060,575
   The Radicati survey was completed by varying sized businesses worldwide, representing a total of  
   228,068 email users.
   February 2012. The Litéra survey was completed by 303 professionals worldwide.
4. Placitella, Chris. “Cos. Gov’t Seek to Keep Lid on Metadata”. Vioxx Plaintiffs  
   News Center. February 6, 2006.
   2003.
   Foundation. July 20, 3007.
   Avanade surveyed 600+ business and IT leaders in 17 countries who challenged common myths  
   about factors driving the Consumerisation of IT.
11. Cisco. “Global IT Survey Highlights Enthusiasm over Tablets in the Enterprise,  
    Shows Customization, Collaboration and Virtualization as Key Features”.  
    January 24, 2012. Research conducted by Redshift Research. 1,500 IT managers and  
    executives in the US, Canada, the UK, France, Germany, and Spain were surveyed in late 2011  
    to assess attitudes, fears and, hopes for tablet form-factor mobile devices (“tablets”) in the  
    workplace.
    March 13, 2012. The ChangeWave Research survey was completed by 1,604 IT buyers.
    Reports. February, 2012.
14. Brownlow, Mark. “Mobile Email Statistics and Use”. Email Marketing Reports.  
    December, 2011.
    Information Technologies”. September, 2008.