

1. News Articles Demonstrate Problems with Electronic Documents

The following news articles show how difficult it is to review and control the content of electronic documents. Most of these security breaches are the result of improper document reviews and not the result of hidden data, but good review procedures and tools would greatly reduce the number of inadvertent disclosures. When you consider how difficult it is to review properly marked material, you can really begin to appreciate the hidden data threat. We have quoted the pertinent text from each article for your convenience.

a. Classified Dutch military documents found on P2P site

At least 75 pages of highly classified information about human traffickers from the Dutch Royal Marechaussee - a service of the Dutch armed forces that is responsible for guarding the Dutch borders - have been leaked to the controversial weblog *Geen Stijl* (No Style).

The documents, which contain phone numbers and tapped conversations, were found unencrypted on a P2P site - possibly Kazaa according to Dutch newspaper reports. The likeliest explanation for their appearance is that a member of the Dutch Royal Marechaussee worked on the documents from home and unintentionally shared his entire hard drive with the rest of the world.

URL: http://www.theregister.co.uk/2005/01/30/dutch_classified_info_found_on_kazaa/

b. 'Confidential US security documents' flaunted online

A Web site has published what it claims are confidential documents from the US Department of Homeland Security relating to possible terrorist activity.

The information appears to have reached the public domain via Google, illustrating how the search engine can be used to uncover links [to confidential information online](#).

The documents contain reports of suspicious activity in the US, such as water supply tampering, an airline pilot being attacked with an axe, and bomb threats.

The documents begin:

"WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of the Homeland Security Operations Center."

URL: <http://news.zdnet.co.uk/internet/security/0,39020375,39185392,00.htm>

c. Iraq battle plan leak sparks overhaul of cybercrime-fighting techniques

The investigation ended in 2003 without finding the source of the leak. But it has prompted changes within the department, which is developing software tools and investigative strategies for computer crime cases that involve large amounts of data, said Lt.Col. Ken Zatyko, director of the DOD's Computer Forensics Laboratory.

The investigation was prompted after details of the U.S.'s planned invasion of Iraq appeared in a series of newspaper articles in the *Times* beginning in July 2002. The articles revealed various

details of the planned invasion and options that were being considered by military planners. Operation Iraqi Freedom was launched in March 2003.

URL: <http://www.computerworld.com/printthis/2005/0,4814,99397,00.html>

d. Office workers careless with documents

The research gathered from businesses across the UK, United States and Australia, showed that as many as 75% of business documents contained legally sensitive information. Also, 90% of business uses had no awareness of "potentially damaging hidden information", such as 'metadata', that is carried with electronic documents.

URL: http://www.nu-riskservices.co.uk/news/articles/cms/1107378394212694732978_1.htm

2. The SRS Electronic Document Security webpage now a public resource

With the release of our electronic document reviewing software scheduled for next week, SRS is now sharing our EDS webpage with the general public. This page is available at:

URL: <http://www.stg.srs.com/eds/>

3. SRS Document Detective scheduled for release on 31 March 2005

The long awaited Document Detective electronic document security scanner will be released as a commercial application next Thursday. For more information about this tool, or to request an evaluation copy, please visit the Document Detective website.

URL: <http://www.stg.srs.com/eds/docdet/>

Please feel free to forward this message to other Government personnel you believe would benefit from this information.

This newsletter is dedicated to raising awareness about the Desktop Publishing Threat to Information Security and to disseminating information that will help mitigate these risks. Our newsletter is published aperiodically when there is news to report. We will not clutter your inbox with idle chatter when there is nothing significant or useful to say. This newsletter is available free of charge to Government personnel and to certain contractors responsible for the generation and protection of National Security Information. Contractor subscriptions are at the discretion of SRS Technologies.

Suggestions and comments are always welcome. If you do not wish to receive this newsletter, please e-mail us and we will gladly remove you from the list. All EDS related correspondence should be sent to rhackett@stg.srs.com.

For a list of articles and information regarding EDS, please visit our web page: <http://www.stg.srs.com/eds>.

To subscribe or unsubscribe from this newsletter, send email to: rhackett@stg.srs.com

SRS Technologies
Systems Technology Group
500 Discovery Drive

Huntsville, AL 35806

Copyright 2005 SRS Technologies