

### **Navy Exposes Personal Data on Website**

In July, The Naval Safety Center (NSC) reported that the personal information of over 100,000 Navy and Marine Corps air crews, including their social security numbers, had been inadvertently published on its public website. This information was contained in four spreadsheets that have since been removed from the website.

While the Navy investigation has not yet published a cause, this incident can be attributed to improper review techniques and hidden data. Data can be hidden in plain sight. Human nature focuses on the data we expect to find and ignores peripheral information that is not perceived as pertinent. The personal data was probably visible in the spreadsheet, but it was easily overlooked because the reviewer was not looking for it. This is why an automated review tool like Document Detective is needed.

Document Detective rigorously reviews the electronic document to root out and expose all of the hidden data it contains. Document Detective examines more than 100 different types of hidden data in Microsoft Word, PowerPoint, and Excel. The next release of Document Detective will include enhancements to our keyword scanner that will detect the presence of social security numbers and other highly structured data in electronic documents. Using Document Detective to review information before it is released can prevent embarrassing situations such as the NSC spreadsheet scandal.

Document Detective should be used to review all incoming documents as well. We've heard several stories recently where local area networks were contaminated by information classified at a higher level than the network. This information was contained in conference CDs and media from other agencies. Many agencies are not doing a good job of reviewing their electronic documents. Don't let their oversight spill over onto your network.

<http://www.fcw.com/article95202-07-08-06-Web>

-----

### **Meta Data Catches High School Cheats**

The Salt Lake City Weekly reported how high school teachers in the area were using the hidden data in Microsoft Word to detect cheating and plagiarism. Like most people, the students are not aware that hidden information is automatically embedded in the documents, and that this data can disclose the origin of the information. Information copied from websites often contains embedded uniform resource locators (URLs) which students do not remove. An embedded URL in the President's Plan for Victory in Iraq shows that the original document had been prepared on a classified system.

Format changes in the document are also indicators of potential plagiarism. Alex Halavais, an assistant professor at Quinnipiac University, said, "When I am reading a document in black, Times New Roman, 12pt, and it suddenly changes to blue, Helvetica, 10pt ... I'm going to guess that something odd may be going on."

[http://www.slweekly.com/editorial/2006/bts\\_7\\_2006-08-17.cfm](http://www.slweekly.com/editorial/2006/bts_7_2006-08-17.cfm)

-----

### **Army's New Best Business Practice Published**

The Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC) recognized Document Detective in their new Information Assurance Best Business Practices (BBP) for

"Data Transfer across Security Domains" that was published in May. The BBP describes Document Detective as, "representative of the technologies and the capabilities that should be included in data transference applications." The BBP also states that Document Detective is not an Information Assurance (IA) tool, which eliminates the need for a National Information Assurance Partnership (NIAP) certification.

03-EC-T-0002, 23 May 06, "Data Transfer Across Security Domains," Version 1.1

-----

### **Information Security Magazine Review**

Mike Chapple reviewed Document Detective 2.0 for Information Security Magazine in July 2006. Chapple described Document Detective as, "an innovative product that assists in the review and sanitizing of Microsoft Office, Adobe Acrobat and other text documents before releasing them outside an organization."

The article says that running Document Detective is simple, and found that our comprehensive tree view of the document contents that highlights potential policy violations works well. Chapple said, "while the entire document tree contains a large amount of information, the policy violation flags helped target our efforts."

Chapple's review did say they found a flaw in processing password protected documents. Document Detective successfully processed the document, but failed when the "Send to App" button was pressed. This was a simple one line fix to the source. If this is the only flaw Chapple could detect, then Document Detective is in very good shape.

Chapple concludes by saying, "Document Detective provides security officials with a powerful tool that incorporates document-review best practices that otherwise require tedious manual checking."

[http://informationsecurity.techtarget.com/magItem/0,291266,sid42\\_gci1196091,00.html](http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1196091,00.html)

-----

### **Hidden data: You may be sharing more than you think**

In August, the Federal Times published an article written by Ron Hackett from SRS Technologies. This article discusses how sharing electronic documents puts the user at risk of exposing sensitive information, and specifically mentions the Ad Hoc Review issue. The Ad Hoc Review feature was added to Microsoft Office XP and 2003 and uses the Excel, PowerPoint and Word's tracked changes feature to keep track of the document review process. To get customers to adopt it, Microsoft turned it on by default. E-mailing a Word, PowerPoint or Excel document using Outlook automatically enables the Ad Hoc Review.

Information-sharing has already created a vulnerability that needs to be addressed. Classified data spills are common, but the problem may be even worse. Because hidden data can be difficult to find, many classified data spills may go undetected.

Federal chief information officers should implement policies and procedures to ensure that documents with classified or confidential data are properly sanitized of all hidden data before being shared. Continuing to do business as usual is dangerous and could be giving our adversaries a tremendous advantage.

<http://www.federaltimes.com/index.php?S=2044545>

-----

## Document Detective Tech Support and Online Store

You can now purchase Document Detective online with a credit card at our new online store. We accept Visa, Mastercard, American Express, Discover Card, and the Government Purchase Card (formerly IMPAC). Go to the Document Detective website at [www.docdet.com](http://www.docdet.com) and click on the purchase link. After entering the billing and shipping addresses, you will be sent to a secure website to enter your credit card information. Orders are usually processed and shipped on the next business day.

The Document Detective technical support website has also been improved. This website is available 24/7 and is available to the public. In addition to informative articles about Document Detective trouble reports, there is general information about securing electronic documents. If you can't find the information you need using our search engine, use the supplied form to contact technical support. Use this form to submit comments and suggestions as well as trouble reports. There is still a private section for our customers to get the latest updates and information that is reserved for our customers. A link to the technical support website appears on the Document Detective website ([www.docdet.com](http://www.docdet.com)).

SRS Technologies is committed to continuing research and product development. While no process or procedure is perfect, Document Detective is the best available solution for reviewing and sanitizing electronic documents, especially when National Security Information is at stake.

Please feel free to forward this message to anyone 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. 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@srs.com](mailto:rhackett@srs.com)

For information about Document Detective electronic document review and sanitization toolkit, please visit:  
<http://www.docdet.com/>

For a list of articles and information regarding EDS, including previous editions of this newsletter, please visit the Document Detective website and click on "The Threat."

To subscribe or unsubscribe from this newsletter, send email to:  
[rhackett@srs.com](mailto:rhackett@srs.com)

SRS Technologies  
Systems Solutions Division  
500 Discovery Drive  
Huntsville, AL 35806  
Copyright 2006 SRS Technologies