

Security Director's Report June 2002

Protect Your Operation From Three Hidden Security Risks

Not every security threat is as obvious as the back door that's propped open or the Post-It with a password that's stuck to an employee's computer. And while most security challenges have solutions, the answers aren't always apparent. See if you're aware of the following risks and solutions:

1. Do people in your organization unwittingly share deleted text? Scenario: A research and development (R&D) employee is working off a sensitive company document but needs to e-mail it to someone, so he deletes the sensitive parts, saves the document, and sends it off. Do you see a potential security breach?

It's certainly possible, if the employee is working on Microsoft Word 97, 2000, or 2002. If the R&D worker is using Word's "Allow Fast Saves" option (also known as AutoSave), the e-mail recipient will be able to see the deleted text if he or she opens the file in a text editor, such as WordPad or NotePad. Microsoft says, "When you save a document with the Allow Fast Saves option selected, Word records only the changes to the document and appends them to the end of the document. This means your document still contains the deleted text, even though it does not appear on the screen."

What to do. The solution is simple, suggests computer consultant Mary Ann Richardson in her recent Techrepublic.com article, "Avoid sending deleted text along with your docs." Notify employees working in Word to go to the "Tools" heading, scroll down to "Options," click the "Save" tab and uncheck the "Allow fast saves" box. That way, Word will always do a full save and remove deleted text from the file. Alternate options include copying and pasting the relevant content into a new document before sending or refraining from sending digital copies of a document altogether.

But deleted text isn't the only information employees may be leaking. Other metadata that you may not want to reveal may also be traveling with Word documents, says Richardson. Information such as: the author's initials, the names of all authors of the document both past and present, document revisions and template information, file properties and summary information, any text or comments that were meant to be hidden, company or organization name, the name of the computer it was created on, the name of the network server or hard disk where the document was saved, and invisible portions of any embedded OLE objects.

Richardson notes there is no foolproof way to completely remove all this information from documents, but you can limit it. Microsoft offers tips in "How to Minimize Metadata in Microsoft Word Documents" on its Web site (<http://support.microsoft.com>). More advice: If your organization provides training classes to computer users, security directors should review those lessons to see if your company teaches such security precautions at the same time it is teaching workers how to use a computer program to improve their efficiency.

2. Do you let European privacy laws stymie your background checks? As we noted a few months ago, experts are still spotting holes in organizations' background checks, including skimping on checks of foreign workers because of the time and expense in getting the info (see, "Are You Still Making These Background Check Errors?" SDR February 2002). But what if the roadblock is the law itself? Some EC countries afford personal data, including credit information, criminal records, driving records, and

official employment records, extensive protection. Is there a way around it?

Yes, according to experts from The Lubrinco Group, Inc. and Financial Examinations and Evaluations, Inc. ("Technical Issues A straightforward approach to getting around European privacy laws in prospective-employee background checks," Business Security e-Journal, April 2002; Lubrinco, New York City; 917-545-9428; www.lubrinco.com). Before hiring, ask the employee to acquire and present to you a "Good Citizenship Certificate." They're not hard for applicants to get and though the exact contents vary by country, they will tell you if the applicant has a clean record or not (though they do not include driving offenses or juvenile crimes). If the job candidate refuses, simply move on to the next applicant.

"[This] is a legal alternative which turns out to be less costly, more straightforward, and which, when combined with proper follow-up, will produce the desired results," according to Lubrinco's report.

Once an applicant jumps this hurdle, check his or her employment record for missing or inaccurate periods of employment, advise the experts at Lubrinco. However, companies should note that this could be tricky because of restrictions placed on European employers. Our advice: Be careful to select investigators who have the skills to uncover a true profile of the employee. Where privacy laws are stricter, the skill of the interviewer becomes more important. To spot less-than-obvious warning signs, he or she needs to: have the appropriate language skills, understand what legal avenues are open, be familiar with the local environment and practices, have skill in reading between the lines of reports, and know the code words that employers in these countries use for poor performance.

3. Is your new wireless network exposing you to snooping? Scenario: Your business has set up wireless connections through its high-speed Internet so roaming laptops and computers can talk on a common corporate network. Or perhaps your CEO has set up a wireless network at home, so he or she can log on from anywhere in the house. Do you see potential trouble? Unfortunately, many companies don't. But by broadcasting your connection, allowing any nearby computer with a receiver to pick up the signal, you may be letting individuals from outside peek in.

What to do. Some experts estimate that more than half of all broadcast points don't have encryption. In this case, an eavesdropper in a car outside can keep tabs on the information individuals are downloading or sending from a wireless network. Security directors need to make sure all wireless base stations have encryption, including those of key personnel working on home wireless networks. It's also a good idea to eschew the basic encryption that come with base stations for newer, stronger encryption technology and to change default mechanisms on base station software to enhance security.

Finally, take note of two other hot scams and put a note in your next company newsletter. Warn employees to:

Avoid ATMs without surveillance cameras. Cases are increasingly surfacing in which thieves rig ATM machines in a small grocery store, for example with tiny devices that read a debit card's magnetic stripe and a thin cover over the keypad which records the users' PIN code as they enter it. After retrieving the stolen data, thieves encode it onto blank cards, punch in the PIN at another ATM, and drain bank accounts.

Delete any e-mail from "the IRS" citing an "e-audit" and requesting immediate information to avoid the assessment of penalties and interest. It's not from the IRS.