Foiling e-document hackers

July 18 2005

A worker sends an office colleague an e-mail with a corporate document attached, but the seeming routine message turns out to harbor a malicious passenger, because the attachment contains hidden pornographic images that were inserted by a hacker during it's transmission over the Internet. When the document is opened by a female employee, she files a lawsuit for sexual harassment.

This particular case is hypothetical, but the situation is real, experts told UPI's Networking.It is something increasingly plaguing corporate networks. To combat the problem, experts said, companies are going to have to monitor workflow, set new policies and install IT to intercept illicit content. The problem is, many companies skip the first step, which involves evaluating work practices and noting how and where secure knowledge is transferred, before investing in IT, said David Drab, director of information content security services at Xerox Global Services. "By conducting a company-wide risk assessment, organizations can identify the information that represents the greatest threat to the company, if exposed," said Drab, who is also a former FBI agent.As soon as the document-management policy is set, company networks need IT to maintain the integrity of documents that flow over the network.

One solution is from a software developer in San Francisco called Workshare.The company's software, Trace! Version 2, is a free metaware utility for Microsoft Office users that automatically alerts them to the risk level of the documents they are about to open. The software scans for sensitive or inappropriate content, both visible and hidden, within electronic documents. "Each year, trillions of documents

are exchanged electronically," said Ken Rutsky, Workshare's executive vice president for worldwide marketing. "There are serious compliance risks and liabilities over the exposure of personal private data, and other sensitive information."

The risks are increased, due not just to potential lawsuits from employees who feel violated by obscene links in a document, but also to certain laws. The federal Sarbanes-Oxley and Gramm-Leach-Bliley acts, as well as the California Breach Law, require that certain information be kept secure for reasons of financial disclosure, intellectual property management, privacy and identity, and related matters.For example, if a document contains the word "confidential" in a header or footer, it probably contains corporate secrets and should be handled with care. If the word is in the text body, it probably is more benign.

Content- filtering software can determine whether the file contains benign or sensitive information before someone opens it.A recent survey of 332 large American enterprises conducted by Proofpoint in Cupertino, Calif., a software security firm, found stopping such leaks was the top concern for those who manage outbound e-mail.More than 35 percent of companies surveyed had investigated a suspected e-mail leak of confidential or proprietary information over the past year.

For example, a proprietary customer list may exist in an Excel spreadsheet, but if the document is converted to a PDF, it might be easier to smuggle it out of the company. So, software developers are developing "audit trails" for individual documents, such as Excel spreadsheets and Microsoft Word word processing files, so each modification to a file can be monitored along the way. The software includes encryption and authentication measures so the "sending and receiving parties can be tracked from start to finish of the transfer process," said a spokeswoman for Tumbleweed in Redwood City, Calif., a maker of enterprise-class secure managed file-transfer software.