Lost Electronic Equipment: *A Loss Prevention Nightmare*

A recent survey of almost 500 employers found that a large majority of companies (81 percent) reported the loss of one or more laptop computers containing sensitive information during the previous 12 months.

The survey highlights the challenges of securing confidential "data at rest," defined as all electronic information found on storage devices within the organization's IT infrastructure. ("Ponemon Institute Releases National Survey on Confidential Data at Risk," PRNewswire, Aug. 25, 2008.)

The study also identified the probability that various storage media are likely to contain unprotected sensitive information.

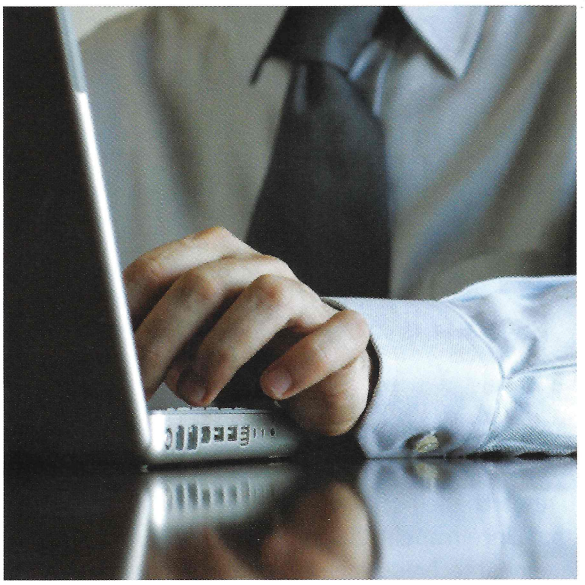
Additional findings from the employer survey include:

- **Loss of confidential data, such as intellectual property, business documents, customer data and employee records, is a pervasive problem.**
- **PDAs and laptops ranked highest among storage devices posing the greatest risk for sensitive corporate data, followed by USB memory sticks, desktop systems and shared file servers.**
- **Sixty-four (64) percent of companies surveyed reported never having conducted an inventory of sensitive consumer information. Sixty-four (64) percent also reported never having inventoried employee data.**
- **Eighty-one (81) percent of respondents reported that protecting sensitive data at rest is a priority this year, and 89 percent anticipated that it would be a priority next year.**

Commentary and Checklist

Employers and emergency service organizations (ESOs) alike face the difficult challenge of identifying and protecting sensitive data in an era of ever-increasing data mobility. Risks posed by loss of data can range from intentional theft to accidental misuse or loss.

Moreover, those who are impacted from security breaches are finding ways to stick liability on those who mishandle their sensitive information, like Social Security numbers. Consequently, employers and



ESOs that demand confidential information from others are required to exercise reasonable care when sensitive information is in their possession.

The Department of Veteran Affairs recently agreed to pay $20 million to settle a class action lawsuit over the 2006 loss of a laptop containing records with personal information of up to 26.5 million veterans and active duty personnel.

Employers and ESOs must make employee, customer and client Social Security numbers a security priority.

Departments that manage customer and client information must make certain that the information is safe from outside and inside threats.

The Federal Trade Commission (FTC) offers an interactive tutorial "Protecting Personal Information - A Guide for Business" that offers low-cost solutions to protecting sensitive data.

According to the FTC, a sound data security plan should include the following steps:

- **Take stock. Know what personal information you have in your files and on your computers.**
- **Scale down. Keep only what you need for your business.**
- **Lock it. Protect the information in your care.**
- **Pitch it. Properly dispose of what you no longer need.**
- **Plan ahead. Create a plan to respond to security incidents.**

This informational piece was originally published on March 25, 2009 on GoGlatfelter.com. Reprinted with permission of The McCalmon Group. This article has been altered with permission of The McCalmon Group for the VFIS audience.