CTSI
Serving Colorado's Counties

Technical Update

Volume 17, Number 1 January 8, 2013

Minimize Risk of Harm From the Loss of Mobile Data Devices

According to a leading employment attorney, a company can be liable if its data system is improperly accessed. As employers and employees grow ever more dependent on portable data tools, preventing the loss of these devices becomes an almost impossible task.

In recent surveys, one-quarter of employees reported lost or stolen smartphones or PDAs and 81 percent of companies reported losing laptops with confidential data. When this happens, all that can be done is to take immediate steps to ensure that the situation is remedied.

Since a virus from a smartphone or PDA could potentially destroy the general system, anti-virus software should be required on all electronic devices. Password protected entry also should be required, so strangers can't access the data.

Employees' ability to put confidential information on laptops, smartphones and PDAs should be restricted — human resources staff, for example, do not need remote access to such data. Employers should have specific protocols in place for authorizing confidential data on mobile devices, and wireless devices should not access confidential information off the network.

Centralizing desktop applications in a secure data center should be done so only one location needs to be secured. When giving telecommuters and other employees' remote access, companies should deploy technology that automatically locks them out if a virus or breach occurs, so one employee's computer problem does not have company wide impact.

What This Means For Counties

Ideally, counties who seek to minimize risk of harm from loss should take security measures such as keeping track of all mobile devices, labeling and registering their inventory and disabling remote access. When an employee who was issued a smartphone or laptop returns it, all data should be stripped from it.

For more information, contact CTSI at 303-861-0507.