Employee Computer Abuse: New Remedy

A March 2006 case decided by the 7th Circuit Court of Appeals involves a remedy that could help employers deal with malicious and disloyal employees who abuse an organization's computer system and data. In *International Airport Centers v. Citrin,* the court found that a departing employee who permanently deleted electronic files from a business laptop could be both civilly and criminally liable under the federal Computer Fraud and Abuse Act (CFAA).

The employee had decided to start his own competing business and deleted work related records, prospect information, and data that would demonstrate his disloyalty and violation of his employment agreement. The CFAA creates liability if someone: "knowingly causes the transmission of a program, information, code, or command, and as a result…intentionally causes…damage to a protected." The court found that the employee's loading of a nonauthorized erasure program on his laptop constituted a "transmission" whether it was done through a CD, internet download, or virus. The CFAA was also violated because the employee was no longer authorized to access company computers as he'd accepted a new job. Similar cases have been decided in Washington, Pennsylvania, and Illinois.

The CFAA is especially useful because it covers both employees and outsiders. It applies to many types of information (not just confidential or proprietary), and is applicable even if no confidentiality or noncompete agreement exists. Unhappy programmers should beware.

Now that laptops, the Internet, and other electronic communication are standard workplace tools related problems will inevitably follow. An understanding of the CFAA and implementing workplace communication policies are critical in protecting key business assets. A few other actions to consider include:

- Implement a comprehensive communication policy that includes discussion of company standards regarding computer, Internet, email, voicemail, and other electronic equipment usage.
- Make certain that data security, access, usage, confidentiality, and related issues are discussed with employees. Consider requiring confidentiality agreements and include these issues in your employee handbook and handbook acknowledgement. Provide regular training as the problems are only increasing.
- Ensure that employees understand that communication systems are company property and are for business use. As such they should have no expectations of privacy and should understand that files, equipment, mail etc. may be monitored, read, reviewed, or disclosed.
- Be prepared to deal with terminating employees and make sure that their access to company systems is limited, turned off or monitored as they're about to walk out the door. Develop a process for the return of company equipment. Establish a termination checklist to guarantee that nothing is forgotten.

info@hrnonline.com
www.hrnonline.com
(800)940-7522