

Shaky Economy May Increase Employers' Need for Computer Forensics

During this tumultuous economy an increasing number of individuals in the workforce have seen their salary reduced, position eliminated or employer shut down. For those still employed, many are experiencing uncertainty and insecurity in their positions. As a result, employers are facing increased risks in many areas, including wrongful termination suits and theft of trade secrets. The use of computer forensics can be a useful tool in dealing with these situations.

Wrongful Termination

Due to the current job shortage, many terminated individuals may be unable to find new employment. Some will seek resolution by filing a wrongful termination suit against their previous employer. Defending wrongful termination claims often includes the use of computer forensics to identify the former employee's activities prior to termination. Establishing a timeline of computer activities can identify productivity issues, policy violations, inappropriate communications to clients and employees and other issues. This documentation may assist in justifying the decision to terminate.

Theft of Trade Secrets

Economic uncertainty has prompted some employees who have not lost their jobs to look for more stable or lucrative opportunities. When new opportunities present themselves, many are more than happy to move on to another employer-and take their previous employer's proprietary information with them. This can be detrimental to the business.

During a recent project, we were engaged by a Fortune 500 company that lost an entire department to their largest competitor. We were tasked with identifying the employees' computer activities during their last week of employment. We identified several employees who had connected USB thumb drives and an external hard drive to

their computers and copied proprietary materials to those devices. More compelling was the fact that one individual's first action at his new employer was to plug one of these devices into his new computer.

The importance of identifying USB devices in theft of trade secrets cases is underscored in *Universal Engraving, Inc. v. Duarte*, 19 F.Supp.2d 1140 (D. Kan. 2007). The judge found it significant that one of the parties used a USB device on the same day he turned in his letter of resignation.

Other items to look for are communications between collaborators, which often include email or text messages with contents such as, "the grass is greener," "moving on," and "I'm outta here." Employees may also use Internet-based email like Hotmail or Yahoo! to circumvent the company's email system when communicating with prospective employers or to send confidential data to their home computers.

If you or your clients suspect that employees have taken proprietary materials, a computer forensics analysis of their computers can often show how and when those materials were taken. This information is not only beneficial in building a case, but also helps identify areas where preventative measures can be implemented.

Contact:

John Mallery, managing consultant
BKD Forensics & Valuation Services
816.221.6300

jmallery@bkd.com