Intellectual Property Protection Using Computer Forensics
Where Does Your Company Data Go?
by Kevin Fagalde and Julie Lewis

Do you know what happens to your company's data when an employee leaves for another opportunity? How much notice did you have that they were leaving? What steps did you take to protect your company's information BEFORE and AFTER that notice was given? What do you do with their computer? You should have answers to all these questions as part of your intellectual property risk management strategy.

The United States Department of Justice estimates that intellectual property (IP) theft cost enterprises $250 billion in 2004. Protecting important corporate data is mission critical to a company's longevity and continued success. Employers have been burned by former employees, whom they erroneously trusted with their company's information. Many employees leave an organization for a legitimate opportunity or lifestyle change and depart only with a general knowledge of your company's information and specific knowledge of the tasks they were assigned while employed, leaving proprietary information behind. Other employees, often recruited by a competitor, will take whatever they can get away with to provide them with a competitive edge at their new employer. Some employees shop for new employment, bargaining with the valuable information obtained in their current role, which may include customer lists, proprietary schematics or designs, source code, financial statements, etc. Which employee described above just gave your company notice?

According to a survey by the American Society for Information Security, the average *Fortune 1000* company reported loss of confidential or proprietary information more than twice a year, with the average loss costing the company more than $500,000. In this digital age, information is easily transferred over the Internet to personal email and online storage accounts, small removable storage devices the size of your thumb, or burned to CD. It is possible, utilizing computer forensic tools, to examine a computer system for evidence that information was transferred to a thumb drive, uploaded to an internet storage site, attached to emails to a personal account, or burned to a CD or DVD.

Have you watched CSI lately? Crime scene forensic investigators spend hours or days at crime scenes collecting evidence because it may be their only opportunity to collect the evidence before it can be altered or destroyed by the elements, tampered with by the suspect, or inadvertently damaged by the untrained novice. Once properly collected, that evidence is preserved for further investigation and can be accessed for examination. Computer forensic examination works much the same way.

Often it is many months after an employee leaves before the discovery of a problem. The key to knowledge of a prior employee's activities is the collection of a forensic image of the data on his or her computer prior to repurposing the computer. When obtaining a forensic image, the source media is protected so that no changes to it occur. A forensic image is a copy of the accessible data areas of digital media, preserving all the data on the media, including deleted files and the dates and times associated with them, as well as portions of deleted files that have been partially overwritten. Once preserved, examination can be conducted on the read-only image to determine if valuable company information has been stolen or improperly distributed.

In this digital age, it should be corporate policy to collect a forensic image of the computer systems of employees upon separation, especially if they are in key roles where your company's data needs to be protected.

What becomes of your company's outdated equipment? Most IT departments reformat the hard drives of outdated computers before they go out the door. Contrary to popular belief, reformatting digital media does not delete data. Rather, pointers to the data maintained in the file system are eliminated. A good analogy would be a library where the card catalog is disposed of, but the books still remain on the shelf.

Several years ago, M.I.T. graduate students Simson Garfinkel and Abhi Shelat purchased 158 used drives. On the 129 drives that were still working, they found thousands of active credit card numbers, along with pharmaceutical records, legal correspondence, and other valuable proprietary corporate information. In addition, 66 of the drives had more than 5 e-mail messages; one had more than 9,500. Less than 10% of the hard drives had been properly and thoroughly cleansed of recoverable data. While few thieves are likely to carry out a recovery effort as extensive as Garfinkel and Shelat's, it is still foolish to think that data on your hard drives donated or sold in the secondary market can't be recovered. In fact, doing so isn't always illegal. The U.S. Supreme Court ruled in California vs. Greenwood that discarded materials confer no right to privacy, giving individuals the right to whatever they find on secondhand hard drives and other storage media.

We strongly recommend wiping of data on computers that will be disposed of and donated or sold in the secondary market. This may occur when an employee leaves a company or because of technology obsolescence. Wiping of the hard drive overwrites all the data on a drive.

As prudent management of a financial institution or a company in another industry with highly sensitive data, it is important to take active measures in safeguarding confidential data and protecting it from those that are not authorized access. Data can contain corporate jewels that must be protected. A risk management plan for data is a critical part of any company's intellectual property protection strategy. Forensic imaging and the wiping of hard drives should be key components of your company's risk management plan.