

What can be done to keep employees from leaving with trade secrets?

When an employee of a business terminates employment, it is customary for the employee to turn in all badges, credit cards and confidential files. What both employers and employees often forget at the time of termination is that the employee sometimes has in his possession company confidential information or trade secrets on his home computer, laptop computer and personal digital assistant.



TRADE SECRETS

PAUL C. VAN SLYKE

It is quite common these days for both technology and commercial business employees to work on their home or laptop computers and to have company confidential business information on the hard drives of their home computers.

Home computers of employees who work primarily from home often contain company confidential information belonging to their employers. Even employees who do not work primarily at home often are given access to company computers via the Internet or telephone lines and have company documents stored on their computers at home.

Hand-held PDAs commonly used by employees often contain names, addresses and notes involving customers, vendors, prospects, confidential projects of the company and company confidential information.

In some cases, engineers or computer programmers have company computer

programs on their home computers, many of which they develop, enhance or edit at home.

CHANGING JOBS

In one case, the chief computer programmer for a small business did most of the coding of a computer program on his home computer for his own convenience. The computer program was later transferred to the computers at the business. The use of this program gave the business a major advantage over its competitors in sales and marketing.

Some time after development of this program, this employee terminated his employment and threatened to sell the computer program on his home computer to a competitor of the business. The employer was faced with the possible loss of its competitive advantage and the devaluation of the design and development costs it had expended on the program. In this instance, the employer was able to persuade the employee not to disclose the computer program to the competitor under threat of suit.

Upon termination, the wise employer will inquire about company confidential information on the home computer, laptop computer and PDA of the employee. If there is a possibility that the employee possesses such confidential information, the employer should request the employee to bring to the office the PDA, home computer or laptop computer for examination by IT staff or a qualified computer expert and to permanently erase any confidential information from the hard drive or PDA.

AVOIDING TROUBLE

A future employer of a terminating em-

ployee is also wise to be careful to ask a newly hired employee about information contained on his home computer and PDA of information confidential to the previous employer.

The employee migrating to the new business could bring confidential information and trade secrets from a previous employer to the new employer that can result in lawsuits brought by the previous employer against both the former employee and the new employer. If so, the new employer should require the employee not to use the PDA in the course of the business for the new employer and to remove the hard drive from the home computer and deliver it to the previous employer.

Of course, the usual problem is that the hard drive on a home computer and a personal PDA contains a mixture of both personal information of the employee that may be private and sensitive as well as confidential information of the previous employer. This mixture of personal and company confidential information can be a sticky problem, especially when delivering the hard drive or the PDA for inspection by the previous employer.

In certain instances, it may be wise for an employee not to mix together personal information and employer's information on the same hard drive or PDA. It is possible, for example, to install a second hard drive on a home computer and use one hard drive for company information and one hard drive for personal information. Another technique would be to use two different computers for personal information and company information at home.

Any employer in this digital age should preferably have written agreements with

the employees. These agreements should provide that company confidential information on home computers, laptop computers and PDAs remain the property of the company even if mixed with personal and private information. The agreements should further provide that the employer has the right to inspect these machines upon notice of termination and to erase all information believed to be company confidential.

If an employee declines to turn over his computer or PDA for inspection, the employer should immediately consider legal options. A lawyer familiar with the law of trade secrets and confidential information can advise the employer of the potential remedies available, the probable costs and chances for success.

The courts sometimes grant short-term restraining orders without notice that requires a terminating employee not to erase or alter information on home computers or to use or disclose that information for the benefit of a competitor. The court will then usually hold a hearing in court to determine whether there is sufficient evidence to extend the order until a full trial before a jury can be held months later.

The employer must act immediately within days of termination of employment to file such a suit and obtain this type of restraining order. If the employer waits more than a few days to file suit, most judges take the position that there is no emergency need to restrain the employee with a restraining order. ■

PAUL VAN SLYKE is a partner in the Houston office of Locke Liddell & Sapp LLP whose practice focuses on intellectual property litigation and trade secrets.