Taking a Byte out of Computer Theft

It is 10:00 p.m. on a Saturday night and the only person in your office is a disgruntled employee that has made the decision to leave your firm and work for a competitor. The soon to be ex-employee e-mails to himself confidential and proprietary formulas, processes, strategies or customer lists - anything of value that can hurt you and help him in his new job. Or perhaps someone from outside your company discovers a back door to your network that allows her to download proprietary financial models your company uses to evaluate its investments.

In the Fall 2005 edition of the *Edge*, I discussed what constitutes a trade secret and how it can be protected. In many cases, the theft of a trade secret or other confidential or proprietary information is accomplished by accessing, transferring or copying information stored electronically. While there are a number of well-recognized claims you can pursue in such a case (i.e., breach of an employment agreement, injunctions, conversion, breach of fiduciary duty or violation of the Illinois Trade Secret Act), there are also a number of less well-known, but equally significant, causes of actions.
specifically created to protect the victim of theft by computer misuse. This article will briefly discuss the statutory remedies available when confidential or proprietary information is misappropriated through computer access.

In 1984, Congress passed the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. While the CFAA was originally intended to prevent hacking into computer systems, it has been expanded to give ""financial institutions"" (a term that is broadly defined) a private right of action in federal court when (among other things) a person:

In one recent Illinois case (2005), Charles Schwab and Company filed suit in federal court against an employee that e-mailed confidential information (such as proprietary investment research strategy and analytical tools) to a future employer, in addition to burning onto a DVD computer files that the employee was only authorized to access to perform his job duties. The court, in allowing the case to proceed, determined that Schwab, as a broker-dealer, constituted a ""financial institution""; that by accessing Schwab's computer network (which serviced more than one state), the employee engaged in ""interstate communication;"" and that the new employer, who would be benefiting from the stolen information, could be held vicariously
liable for the acts of its new employee.

One significant advantage to this remedy, as opposed to an action under the Illinois Trade Secret Act, is that there is no requirement that the misappropriated information be a ""trade secret"" - any information, whether secret or not, can be protected under the CFAA. All the statute demands (assuming its requirements are met) is that the information be located or stored on a computer and accessed without authorization.

Other state or federal statutes that can assist the victim of computer theft include the Illinois Computer Crime Prevention Law (Chapter 720, Article 5/16(d)) and the Economic Espionage Act of 1996 (18 U.S.C. §§ 1831 - 1839). While these acts are primarily criminal in nature, there is leverage to be gained by having these statutes at ones disposal.

Under Illinois' statute, computer fraud occurs when there is access to a computer as part of scheme to deceive or defraud including, but not limited to, the theft of electronically produced data, confidential or copyrighted material or software in any form. These offenses are punishable as felonies. While the statute is almost always used to criminally prosecute a person that knowingly and without authorization tampers with another's computer, at least one court has held that,
under limited circumstances, it can allow for a civil remedy.

Finally, in 1996, Congress, recognizing that vast amounts of information can be stored and transferred electronically and, because of technological advances, done so quite easily, passed the Economic Espionage Act (EEA), making it a criminal offense to steal a trade secret. This statute requires proof of intent to convert a trade secret, economic benefit to someone other than its rightful owner, and the knowledge that the offense will injure the secret's owner. In passing the EEA, it was Congress' intent to prohibit every type of trade secret theft ""from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each others bid proposal, to the disgruntled former employee who walks out of his former company with a computer disk full of engineering schematics."" H.R. Rep. No. 104-788 (1996).

While the EEA cannot be used by anyone but the federal government, it is an arrow in the quiver. In one recent case, the U.S. Attorney's Office for the Northern District of California prosecuted and obtained a conviction against an individual for copying, without authorization, computer files relating to the design and testing of a microprocessor. The
person charged knew the materials contained trade secrets and copied them with the intent to convert them to his own economic benefit at his new place of employment. In imposing a two-year prison sentence, the court emphasized the importance to our economy of protecting intellectual property of a significant value.

Trade secret protection is, in part, accomplished by aggressively protecting your confidential or proprietary information and by bringing maximum pressure to bear on those that misappropriate your intellectual property. These statutes, in addition to the more well know remedies, may help you achieve that goal.

"