# New law offers relief for hacked employers

## Computer Fraud and Abuse Act creates a civil remedy for private businesses victimized by employees

COMPLIANCE CORNER

Richard Hunt

Many companies are concerned about the best way to protect their electronically stored information and prevent it from being accessed, altered or deleted by unauthorized individuals. In some cases, these "hackers" can be the company's own employees: Either during employment or on their way out the door, they exceed their access to the company's computers and wrongfully obtain company information. While companies have long been able to bring suit in state court for this type of wrongful conduct, a relatively new law allows employers to seek relief in federal court.

In 2008, Congress passed a federal statute that creates certain risks for employees and provides employers a right to file a lawsuit in circumstances in which employees have engaged in unauthorized use of a company's computer system and the information stored on company computers. Although the legislation is commonly used by federal enforcement agencies to prevent fraud and related activity in connection with computers, it also creates a civil remedy for private businesses.

The Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access of any protected computer that causes damage or loss. An employee risks violation of this federal statute when he or she accesses a protected computer without authorization or exceeds authorization granted, and knowingly and with intent to defraud obtains anything of value and causes the loss or damage in any one-year period aggregating at least $5,000 in value.

Employees risk being subjected to litigation under this federal statute if, among other things, they access without authorization their employer's computer system and the information stored therein or exceed the authorized use or otherwise obtain unauthorized access by using another person's password or engage in hacking in order to obtain information.

Employers can guard against unauthorized use of their company computer systems by drafting and having employees execute a computer operating policy or agreement. It should spell out the scope of the employee's authorized access, the duration of use, and prohibit employees from sharing or borrowing passwords.

**Employers can guard against unauthorized use of their company computer systems by drafting and having employees execute a computer operating policy or agreement. It should spell out the scope of the employee's authorized access, the duration of use, and prohibit employees from sharing or borrowing passwords.**

However, even in the absence of written agreement, employers can still seek relief under the federal statute if they have taken steps to limit or curtail an employee's access to computers. For example, when an employer discharges an employee or receives notice that an employee is quitting, in many circumstances it should at this time cut off authorized access to the computer and make it known to the employee that the employee no longer has consent or authority to access the protected computer system or the information stored on the computer system. A departing employee who finds a way to avoid this directive and gain unauthorized access to the company's computer system may be sued under the federal statute.

The federal statute does require that an individual who intentionally accesses a computer without authorization or exceeds authorized access must cause damage or loss in excess of $5,000. Under the CFAA a "loss" includes any reasonable cost to any victim, including the cost of response to an offense, assessment of damage, and restoration of the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute. Thus, it is not necessary for data to be physically changed or erased in order for a company to show that it has suffered a loss or damages. It is sufficient to show that there has been an impairment to the integrity of the data, as when an intruder retrieves password information from a computer, and the rightful computer owner must take corrective measures to prevent the infiltration and gathering of any confidential information on the computer.

Of course, as mentioned previously, if an employee had authorized access to the computer and upon separation from the company retained trade secret information, or confidential information, then the company may have various claims under state law, including misappropriation of trade secrets under the Uniform Trade Secrets Act, breach of contract, breach of fiduciary duty, conversion and interference. But when an employee does not have authorized access, the CFAA permits a company to sue in federal court – where the company can seek not only damages, but injunctive relief as well.

There may be some strategic advantage to companies filing suit in federal court as opposed to state court. Attorneys retained to represent individual employees who reside in small towns or rural areas often prefer to be in the state circuit court where the individual resides.

In contrast, companies headquartered in big cities or in different states frequently want to have the option of commencing the litigation in federal court. Lawsuits brought under the CFAA give the federal court jurisdiction over all claims, provided one of the actions states a claim under the CFAA.

Therefore, it is important that employers keep this statute in mind when considering their options against an employee who has exceeded his or her authorized access and obtained company information.

*Richard Hunt is an attorney with Barran Liebman LLP. He has more than 30 years of experience representing employers and executives in matters relating to non-competition and nonsolicitation agreements, confidentiality obligations and trade secrets, and litigation between employers and their former employees. Contact him at 503-276-2149 or rhunt@barran.com.*