CASE STUDY

Cadence Design Inc., a U.S. chip maker, filed a lawsuit in 1995 after learning that one of its engineers had stolen Cadence's proprietary sourcecode shortly before leaving the company. Cadence's IT department noticed that large amounts of data had been transmitted out of the company's system, which alerted them to the wrongdoing. Investigations into the incident revealed that the engineer had stored proprietary software on a personal computer, and the pirated software was being incorporated into products sold by a competitor. Coincidently, the competitor company, Avant, was formed by four other former Cadence employees. A copyright infringement lawsuit was filed by Cadence claiming that the former employees had stolen the sourcecode to start the new business. Additional securities fraud class actions were filed by shareholders and a criminal suit was also brought against the former employees. Experts carefully documented forensic evidence obtained from network logs at Cadence and the hard drive in the employee's personal computer before bringing the case to trial. Further evidence was obtained when comparisons of the sourcecode used by Cadence and Avant revealed that the error codes designed into the code at Cadence were duplicated in the code that Avant was using in their products. Avant has since settled the class action lawsuit for $47 million and on May 22, 2001, pled no contest to charges of stealing the trade secrets from Cadence. As a result of the plea agreement, Avant agreed to pay $27 million, plus restitution. The individual employees involved in

the theft of sourcecode will pay $8 million in fines and serve jail sentences ranging from one to six years.

The trial reflects the importance of trade secrets, and in today's competitive climate, trade secrets may be all that differentiates one company from another, thus enhancing the need for security. It's not uncommon these days for one company to try to steal an employee from another with the offer of greater competition in the hopes of removing the asset from being available to the competitor, and also that the employee will bring trade secrets that can be exploited by the competitor. At the same time, this practice gives rise to lawsuits between rival companies. Recently, Compaq and Trident Microsystems have filed similar lawsuits against competitors claiming trade secrets were stolen. More unusual in the Avant case is the tough sentences handed down against the employees involved in the theft, but even these cases are becoming commonplace.

Confidential company information does not always involve high-tech gadgetry. Recently, the New Jersey Supreme Court ruled on behalf of an employer who had filed suit against two former employees for stealing client lists and customer data. Similar to the Avant case, the employees decided to leave their employer and open a competing business. While they still had the trust of the current employer, they secretly gathered information regarding specific client accounts. Within several days of the employee's departure, all of the clients whose data had been obtained had gone with the new firm.

Certainly the employees involved must have had a good working relationship with the clients, but the data the employees used from their former employer was legally protected since it was obtained by the employer during the course of employment and was to be used for the sole purpose of serving the client. The employer filed suit, and the court ruled that the former employees had breached their duty of loyalty and competed unfairly because they had actively sought to harm their employer's business to provide a competitive advantage.

1. What steps can companies take to protect trade secrets?

2. With more persons working from home, how does one separate data intended for the employer from what might be considered personal property?

3. What policies could be put in place to ensure employees adhere to safe guidelines regarding the use of confidential company data?

SOURCE: Based on CNET news, "Avant trade secrets trial to begin," March 14, 2001.