CSO The Resource for Security Executives
csoonline.com Home | Magazine | Newsletters | Career | Online Features | Resources | Search

June 2004 *CSO* Magazine

Flashpoint

Open Secrets

Can you still claim your trade secrets were stolen if your security was sloppy?

BY WILLIAM COOK

TIME WAS, A COMPANY could feel that their trade secrets were reasonably safe if they were stored in a password-protected computer system. Most courts agreed. However, a court opinion rendered in 2002 in Arkansas found that one company's sloppy password controls left its most-prized information vulnerable.

The case of *Weigh Systems South v. Mark's Scales & Equipment* involved two former Weigh employees—a manager who started a competing firm, Mark's Scales & Equipment, and a service technician who joined him at the new company. Weigh alleged that its former employees stole proprietary information on their way out the door.

Weigh filed a complaint seeking damages and injunctive relief, alleging that the former employees and Mark's Scales violated the Arkansas Trade Secrets Act. Weigh asserted that its former employees had misappropriated its customer and vendor lists, pricing information, software, service agreement inventory checklist and marketing plans—all of which constituted trade secrets. Looks pretty good for Weigh so far...right?

The key question was, Is such information protectable as trade secrets? The court identified several factors material to its determination of whether information is a trade secret. These factors include: 1. the extent to which the information is known outside the business; 2. the extent to which the information is known by employees and others involved in the business; 3. what measures were taken by the company to guard the secrecy of the information; 4.

the value of the information to the company and to its competitors; 5. how much effort or money the company expended in developing the information; and 6. the ease or difficulty with which the information could be acquired or duplicated by others. The evidence presented in court was not favorable to Weigh's case.

■ Weigh conceded that some or all of its customer lists and vendors appear in public directories or are available on the Internet. The testimony at trial established that Weigh's marketing plan was established by visiting trade shows and talking with customers about upcoming projects.

■ The court also found fault with Weigh's security practices. The court observed that when Weigh technicians installed Weigh software, they were supposed to change the default password to one that only Weigh employees knew, but they did not always follow this procedure. The testimony further established that it was not uncommon for employees of Weigh to provide customers with the Weigh password. There was also testimony that a computer bug existed in Weigh's software that allowed customers to gain access to the program without using any password, and that Weigh did not swiftly act to correct the bug.

■The value of the information, to both competitors and to the company, was also difficult to determine. Weigh did not provide evidence as to the value of its vendor list, pricing information and so on. Instead Weigh contended that this information had been developed over time and was essential to making quotes on jobs and installing equipment.

After reviewing the facts, the court concluded that the information Weigh sought to protect was not a trade secret. It specifically concluded that the information contained in Weigh's so-called trade secrets was information that was generally known or readily ascertainable. It further held that Weigh did not take adequate steps to protect certain information from being acquired or duplicated by others. Because the information was not a trade secret, the court concluded that the former Weigh employees and Mark's Scales did not misappropriate the information from Weigh.

What do we draw from this case? First and foremost, your "adequate" security requirements change with time. You need to keep current on the technology, the case law and the regulations that apply to your business community. The adequacy standards that apply will vary between industries. Second, if your company brings a trade secret action against anyone, you, as the corporate security officer, will be a prime witness for the other side. You will be questioned at length in depositions and at trial about security practices you used and didn't use with respect to your company's trade secrets. Be prepared. ■

— Learn More —
In the Risk Measurement and Analysis Research Center

William Cook, a partner with Wildman Harrold Allen & Dixon based in Chicago, specializes in intellectual property litigation, business continuity and security. Cook is also president of InfraGard-Chicago and a founding member of the U.S. Secret Service Chicago Electronic Crimes Task Force.

add a comment:

Name:	
Title:	
Corp:	
Email:	
Subject *	
Your Comment: *	

* Required fields.
Selected comments may be published in *CSO* magazine.
We will neither sell nor display your personal information.

Send Comments

CSOonline.com
The Resource for Security Executives