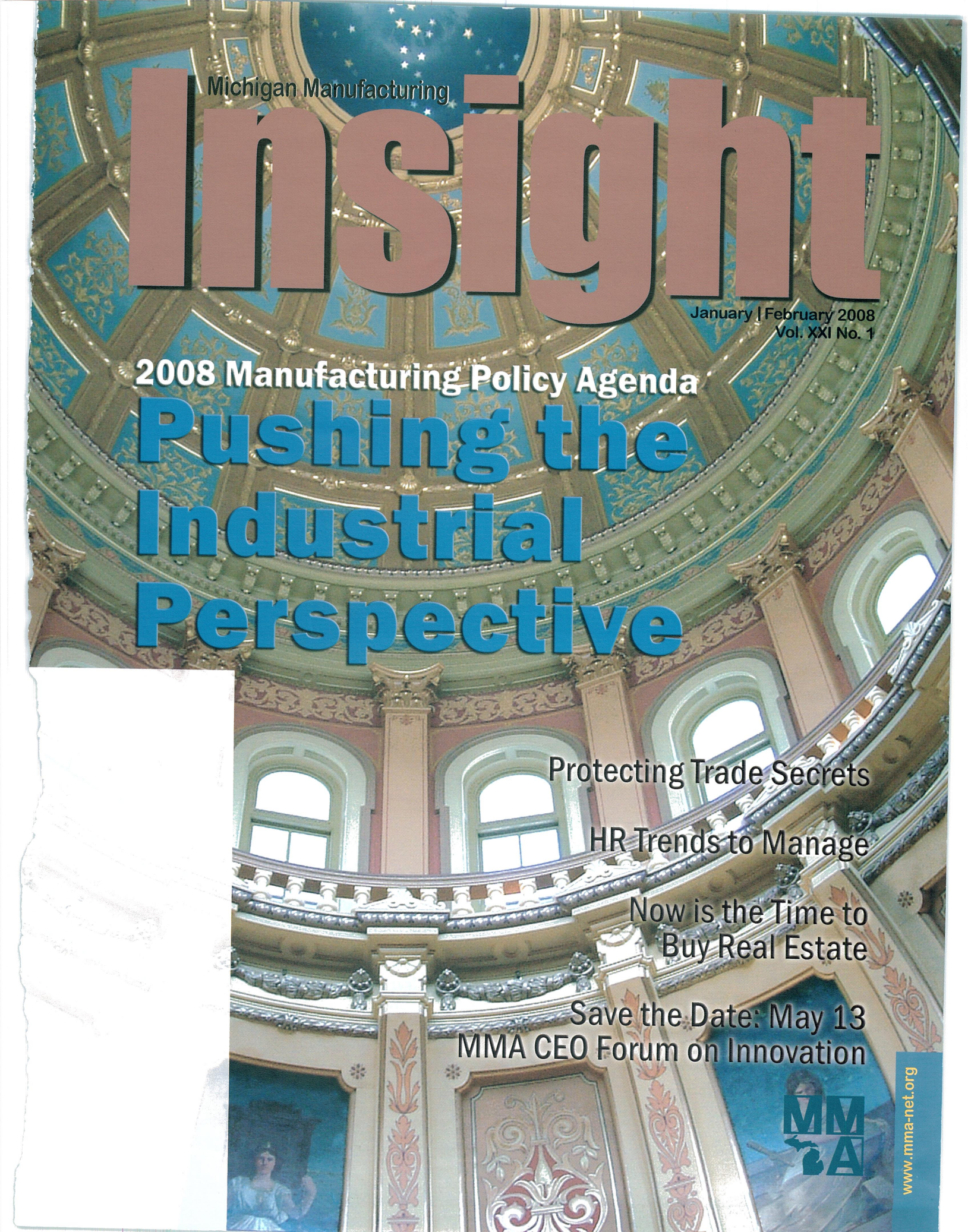


Michigan Manufacturing

Insight

January | February 2008
Vol. XXI No. 1

2008 Manufacturing Policy Agenda

Pushing the Industrial Perspective

Protecting Trade Secrets

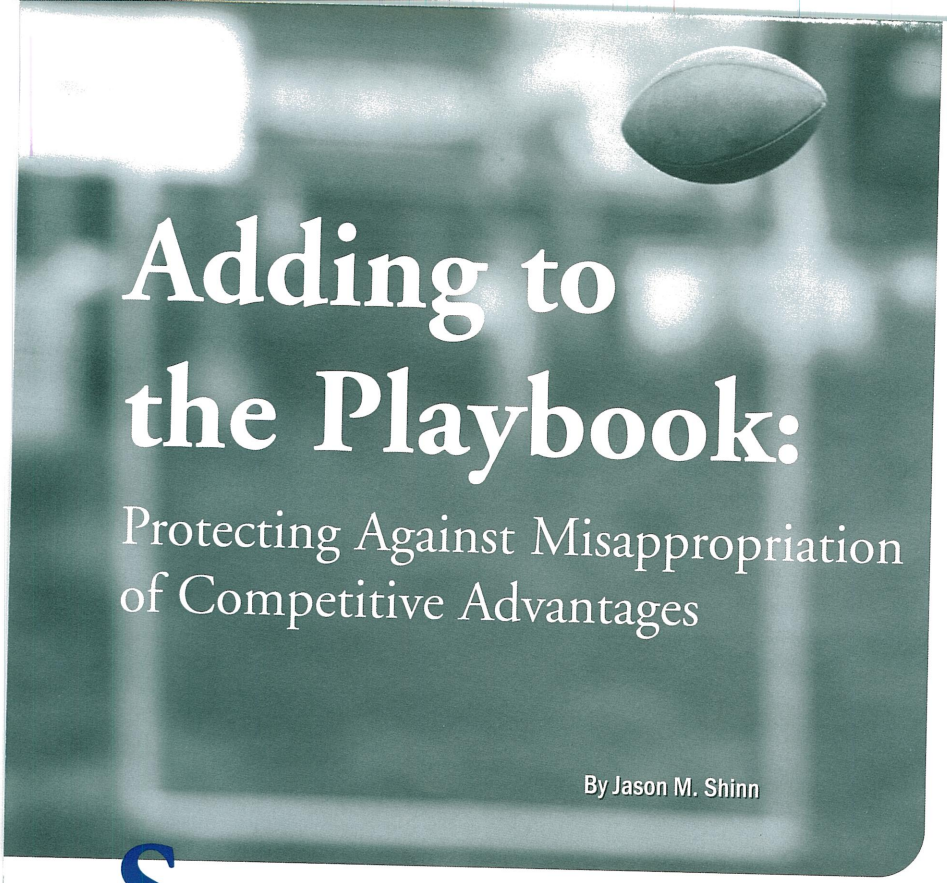
HR Trends to Manage

Now is the Time to Buy Real Estate

Save the Date: May 13
MMA CEO Forum on Innovation

MMA

www.mma-net.org



Adding to the Playbook:

Protecting Against Misappropriation of Competitive Advantages

By Jason M. Shinn

Sports franchises depend on talent within the organization to win. Similarly, companies depend on competitive advantages known only within the organization to achieve success. Indeed, it is estimated that U.S. companies spend trillions of dollars annually to develop such advantages.

It has also been estimated that U.S. companies lost between $59 and $300 *billion* due to misappropriation of their intellectual property (IP) over a three-year period.

Accordingly, many companies have taken steps to implement a trade secret protection plan or other measures to protect their investment in developing IP and the competitive advantages provided by their IP in the marketplace.

Trade secret protection — a good defense is not always the best offense

In Michigan, to establish a trade secret generally requires showing that the information is **valuable** and **reasonable steps** to guard the secrecy of the information were taken. Under Michigan law, the essence of a trade secret is that it derives its value from secrecy.

Thus, regardless of the value of the actual information, failure to take reasonable measures to protect its secrecy will defeat any claim for trade secret protection.

For instance, in the case *Weigh Systems South, Inc. v Mark's Scales & Equipment, Inc.*, it was ruled that the plaintiff's information was not a trade secret because the company did not take adequate steps to protect information consisting of customer, vendor and pricing list; marketing plans; and computer software.

Unfortunately, without proper IP protection measures, companies can be blindsided by a "Monday morning quarterback" determination that sufficient measures were not taken to protect the secrecy of the claimed trade secret. This determination, however, comes only *after* a company's IP has been misappropriated, leaving organizations to scramble to make something out of a broken play.

But companies may still have the opportunity to protect their competitive position by adding a play to protect IP under the Computer Fraud and Abuse Act (CFAA).

Going on the offensive with the CFAA

The CFAA is a federal statute that was first passed in 1984 as a criminal statute and amended in 1994 to allow for civil lawsuits. The CFAA generally applies to computer-related technologies used in interstate commerce and protects against the unauthorized access to information stored on such technologies.

For companies, the most likely claim against an unscrupulous employee who has misappropriated company IP requires showing that the former employee (i) accessed a "protected computer" i.e., one that is used in interstate commerce; (ii) without authorization or in excess of authorization granted by the employer; (iii) "knowingly" and with "intent to defraud"; and (iv) as a result has "further[ed] the intended fraud and obtain[ed] anything of value."

Courts have generally held that an employee's "authorization" ends or was "exceeded" when the employee engaged in conduct contrary to the employer's business interests, e.g., competing directly against the employer or benefiting a new employer (as in *Airport Centers LLC v Citrin* and *Shurgard Storage Centers, Inc. v Safeguard Self Storage, Inc.*).

But, in *Lockheed Martin Corp. v Speed*, a Florida court declined to follow the *Shurgard* and *Citrin* decisions and ruled that an employee who copied computer files before departing for a rival firm was neither "without authorization" nor "exceeding authorization" under the CFAA because such access occurred while the employee still enjoyed access privileges to the company's computer system.

And, in *B&B Microscopes v Armogida*, a Pennsylvania court rejected "any contention that [the employee's] conduct in accessing the laptop computer provided to him by B&B and deleting and/or overwriting B&B business files constitutes" unauthorized access under CFAA because the employee had authorization to use the laptop in question.

The reasoning for bringing a CFAA claim against former employees was underscored by one court, in *Pacific Aerospace & Electronics, Inc. v Taylor*, as follows:

> Companies frequently find themselves in litigation with former employees who depart to set up shop elsewhere in competition with their former employer. Such former employees may attempt to gain an edge for their new venture by making use of proprietary information, such as customer lists or trade secrets, obtained with ease of access from their former employer's computer database or workstations that are linked together in a network. While passwords and other electronic means can limit the unauthorized dissemination of some confidential information, an employee who has not yet announced his departure is still able to access confidential information and store it on a CD or floppy disk before he or she leaves. Computers also make it easy for employees to quickly transmit information out of the company via e-mail…Employers, however, are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system.

Executing a winning game plan using the CFAA

The complex statutory requirements and strategic considerations for bringing a CFAA claim are beyond the scope of this article. But what is important for companies to remember is that under the right circumstances the CFAA may provide an opportunity to bring a federal lawsuit to obtain injunctive and monetary relief against a departing employee — and the departing employee's new employer — without having to confront the procedural and evidentiary hurdles posed by traditional trade secrets and unfair competition laws.

This is because the CFAA's focus is on the acquisition of the information by improperly accessing or exceeding authorization of a computer system.

This wrongful acquisition relieves a company from proving the information wrongfully accessed constituted trade secret, confidential or proprietary information to support its CFAA claim.

Also, a company need not show that the former employee breached an employment, confidentiality or noncompete agreement.

Lastly, no showing that the former employee is actually using, or threatening to use, the information is required.

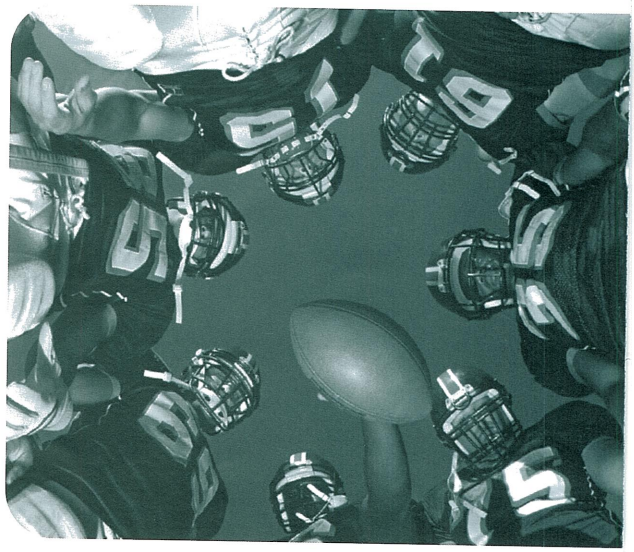
Further, adding the CFAA to a company IP protection playbook requires "off-season" preparation. That is to say, companies must have in place plans for preserving the necessary evidence to support a CFAA claim, which will generally reside on computers, server logs, e-mails, etc. Such evidence is infamously easily lost or altered.

In *PC Yonkers Inc., supra*, for instance, the plaintiff failed to submit sufficient *admissible* evidence from the company's computers to obtain a preliminary injunction under the CFAA.

Post-game review

It is not necessary to have the budget of a big-time sports franchise to implement a winning IP game plan. But developing a game plan is absolutely necessary as companies cannot afford to lose their competitive advantages to "free agency."

Accordingly, companies should develop a defensive IP protection plan with an experienced legal "coach," enforce whatever plan is implemented and regularly examine that plan against technological and legal developments to *respond* to risks rather than *reacting* to a crisis.



And if these defensive efforts are not enough, companies should be ready to go on the offensive with the CFAA. ■

Jason M. Shinn is an attorney with Lipson, Neilson, Cole, Seltzer & Garin, P.C., where he handles claims relating to breach of contract, theft of trade secrets, the CFAA and various business torts. He can be reached in the Bloomfield Hills office at 248-593-5000 or jshinn@lipsonneilson.com.