



370 Southpointe Boulevard  
Suite 310  
Canonsburg, PA 15317

Phone: 724-743-4242  
Email: [info@us-mindmatters.com](mailto:info@us-mindmatters.com)  
Website: [www.us-mindmatters.com](http://www.us-mindmatters.com)

## ***Intellectual Property:*** **A Mythical Case History about Trade Secrets** **(second of two articles in a series)**

By Keith Cochran, MindMatters Technologies, Inc.



The knowledge economy enterprise has a secret about its secrets: it often knows very little about them!

The enterprise is rigorous and granular when it comes to tracking trucks and pencils, but soft and open-ended with trade secret and proprietary assets that are the lifeblood of the modern enterprise. And the enterprise is paying: \$59 billion in trade secret theft for the Fortune 1000 in the year ended June 30, 2001, according to PriceWaterhouseCoopers, in a survey for worldwide security organization ASIS International; and median legal costs of \$500,000 per incident for trade secret disputes (survey of IP lawyers by the American Intellectual Property Law Association). Not to mention the lost opportunities to find good ideas and expertise faster, share knowledge, evaluate and prioritize.

To illustrate the problem, and offer a solution, let's follow a secret into a mythical enterprise, reviewing what would happen to it now, and what could or should happen to it when proprietary assets are managed the way they could be.

### **Project Animate!**

You can only do custom sound animation effects in PowerPoint using .WAV formats. Many popular, common non-.WAV formats exist, but that none of them will work if you want to create custom sound animations in PowerPoint.

Now, let's assume that "Fred" discovers how to convert files in unusable formats to the

only usable one, enabling him to fly through PowerPoint sound animations in seconds! (Fred's secret isn't a patent, or trademark or copyright. If creating unusual PowerPoint presentations were an industry instead of an everyday activity, he would have a classic trade secret. In fact, Microsoft tells users in a very inconspicuous way that they must use .WAV files, probably denying "secrecy" status. But this is a very trade secret-like discovery, so let's assume that Fred's secret is a bona fide trade secret/proprietary asset.)

Let's also assume that Fred works for a large company that offers consumers a utility program allowing them to enhance their PowerPoint presentations. Fred's contribution could create a helpful area of functionality allowing users to embed any sound in any format, so they don't trip over the .WAV file issue. To the extent competing programs did not contain this functionality, Fred's secret would contribute to an advantage held by his company in the marketplace. Competitors hoping to provide this same functionality would need to duplicate Fred's trials and errors themselves – or take other actions, lawful or unlawful.

### **A Typical "System"**

Let's now consider how this discovery would be managed by Fred's company – which makes software solutions and whose market cap depends on knowledge assets giving it competitive advantages over others. If this

mythical company managed Fred's proprietary asset as the typical enterprise does, Fred would create his secret, but would have nowhere to put it – no central repository would exist for him to submit his creation for safekeeping, evaluating or fast-tracking, or for dissemination to others who may be able to make use of it. He would simply hand it to his manager. What his manager did with it, Fred may not even know. He would likely get no specific feedback that his discovery was a protectable trade secret that he should be careful not to disclose except under circumstances in which its confidentiality can be preserved.

(In a survey of attitudes included in the ASIS survey, no reporting company that experienced IP losses agreed with the following statements: *Employees know where to find answers to information questions; the digital forms of our trade secrets and proprietary information are at least as well protected as the hard copy sources of the information; and our law department works closely with the information systems and security staff to help identify and protect the digital forms of trade secrets and proprietary information.*)

Thus, Fred might talk casually to peers about it, or send it to others in emails. He would not warn these others about what they could do with his secret once he disclosed it to them. For its part, the corporation would not have any way to track the existence of Fred's secret, or to follow its trail within the corporation to any others he spoke with. The ASIS survey points out that "in far too many organizations, [proprietary assets] are not tracked in corporate accounting systems."

From a strategic management standpoint, the company would have no list of what secrets and ideas exist, so there would be no way to take stock of them, or compare them to one another, or evaluate Fred or his department against other departments. There would be no way to find and share ideas in a planned manner. For example, let's say that a new Excel initiative was being spearheaded by Fred's colleagues in the Schenectady office. The project involved new techniques for embedding custom animation effects in Excel documents – for which Fred's discovery was

directly relevant. But his discovery had never gone into any enterprise-wide database. In addition, since the marketing people that dreamed up the Excel initiative didn't have any such database to target messages to, they didn't make any effort to find Fred, and he never found out about them or their "Excel Initiative." Unless memos and emails somehow made it to his colleagues in Schenectady, they would just labor on themselves, and offer an Excel product without Fred's functionality or "discover" Fred's secret for the second time!

Now, fast-forward to when Fred decided to leave the company. He would announce his departure, and, if the corporation was reasonably well organized from a human resource standpoint, he would be given an exit interview or briefing. Part of that briefing might involve a warning about trade secret matters – one of the typical tools used now to prevent misappropriations. The corporation would have no idea what Fred worked on or what secrets were created within his department or geographic unit. It may have been years since he made his discovery, his superior could be someone new, he could have been transferred to a new office or offices, etc. Thus, the best the corporation can do would be to admonish him: "Don't take any company secrets." Fred might ask, "What are the trade secrets I shouldn't take?" The company wouldn't specify them because it wouldn't know.

Following his departure, Fred would typically seek employment in a related industry, an area in which he was familiar. Now, if Fred was truly evil, and intended to divulge his secret to a competitor, the corporation's systems wouldn't even know to react. It would have no watch list matching breakthroughs and proprietary assets with specific people. Crime would pay and Fred would get off scot-free. More likely, though, Fred isn't evil, but is a conscientious individual and would not knowingly reveal anything he knew to be a secret. For these inadvertent disclosures, which constitute a large part of trade secret disclosures, the whole thing could have been avoided if the corporation had only told Fred what the secrets were!

## From Bad to Worse

Now, the lawyers take over. No record exists of what people worked on in the company. Instead of a scalable, preemptive, thorough, comprehensive and inexpensive (compared to litigation) management system for proprietary assets, the attorneys create a kludged, partial, extremely expensive "record" to deal with a single trade secret issue. The main focus of activity – recreating the past. They use discovery to decide what Fred's secrets were. They find his manager and co-workers – maybe at other employers – hit them with deposition notices, and in a mere 100-200 hours (at lofty hourly rates) determine that Fred knew something about a unique method of creating custom sound animations using .WAV files! With another 100-200 (to 1000) hours, they decide how to establish that he knew this, and then revealed them to his new employer. Then they spend even more countless hours trying to prove that his secret was a secret and to build their case and surmount procedural, legal and factual hurdles. Fred spends hundreds or thousands of hours; so do all of his current and former bosses and managers.

And the result? Fred might be evil, and the result might be that the corporation wins. So the best result is that it spends hundreds of thousands of dollars to get the same result it could have gotten, in many cases, with a simple briefing as Fred left. But it could well lose - how does it really prove that it kept Fred's secret under wraps? Its lack of systems may be characterized as a "decision" to put the secret into the public domain, thus denying secrecy status and depriving the company of a remedy. If Fred is just the wrong guy, or hasn't revealed his secret or been hired in an area where it's not relevant, then he's extremely bitter about the whole thing and tells all his friends never to work for his former employer. If Fred is innocent and the employer still wins, it spent all that money to obtain a meaningless injunction preventing his employment by a competitor when he didn't even threaten it.

Thus concludes a case study of the life of a trade secret asset at a typical enterprise in

today's knowledge economy! Hardly an optimum, efficient system for managing the proprietary assets and ideas of an enterprise.

## A Better Way

What should happen? Some thinking is beginning to emerge that is based upon the needs of the enterprise, the unique importance of these assets, and the rational allocation of resources to manage them effectively. The result is a rational proprietary asset management system. The system would be akin simply to an accounting system for this critical class of assets that brings to them the same accounting system visibility that other systems bring to physical assets or cash or customer relationships.

In Fred's case, the enterprise should have made better use of its investment in him. The key to doing so is a system that manages his idea from the point of creation throughout its useful life in the enterprise. The first task would be to identify what the assets are. The enterprise should treat Fred's idea about .WAV files as the asset-creating event that it is. It should tell him that this is a secret and what he needs to do to preserve its status as such. It should route his secret to his manager and anyone else the manager feels is appropriate. It should tell Fred who has privileges to see his secret, and how/where he should talk about it.

The system should track where Fred's secret goes within the enterprise. It should facilitate judicious sharing of the secret with Fred's colleagues in other offices, by creating a protected environment in which Fred or a manager can make it available for others that may wish to use it, without sending out an inappropriate and ineffective broadcast email. The enterprise should be specific with Fred when he leaves, letting him know what he worked on – specifically! – and pointing out whatever work product is protected.

Within the corporation, Fred would know to be careful. He would have a place to put proprietary assets. The secrets and know-how would be known for management purposes, searchable by colleagues or managers seeking to locate expertise. The corporation could tell,

and control, who viewed them. And when Fred left, the ideas would be there in all their specificity. Fred would know exactly what he couldn't talk about. If, indeed, he were evil, he would know the corporation was watching and would have a definitive record of what he worked on. More likely, if Fred were innocent, and just needed to know what not to do, he would know. Disputes would diminish dramatically.

There is an art to creating such a system. Fortunately, practitioners of this art are emerging, providing large enterprises with the holistic tool sets, targeted to this class of assets. One example is MindMatters Technologies, Inc., a solutions company with successful implementations in companies including PPG Industries, ITT Industries and public device company Respiroics, with several more installations set to proceed.

## Conclusion

What companies do to manage and protect proprietary assets will be scrutinized more and more carefully as the industrial enterprise of yesterday, with its truck fleets and physical inventories, gives way to the knowledge- and intangible-based enterprise of today and tomorrow.

Proprietary assets of the modern knowledge enterprise *must* be managed with the same granularity as physical assets. They require "locks and keys" and security in every sense that their physical counterparts do – perhaps even more so since they are so portable and liquid. But these need to be tailored to the unique characteristics of proprietary assets and the threats that imperil them. Fortunately, relatively easy and inexpensive steps can accomplish a great deal, especially in savings related to fewer disputes.

And once these steps are adopted, Fred, his employer, and industry itself, will all be better off!

*Keith Cochran is a strategic advisor with MindMatters Technologies, Inc., a solutions company dedicated to helping companies preserve, protect and profit from innovation and intellectual property assets.*