

Saving Intellectual Property

By John Avellanet, Managing Director and Principal of [Cerulean Associates LLC](#)

Reprinted with permission from SMARTERCOMPLIANCE™ 2(2): p 1,4-5 (February 2008)

Patents, trade secrets and confidentiality agreements are mere words on paper to the scientist, engineer or executive intent on deception and theft.

And if you have outsourced your research and development efforts overseas to countries with unenforced intellectual property laws and cultural norms that ignore individual property rights, then the intent to deceive and thief isn't even present—in their eyes, your intellectual property already *is* their intellectual property.

Rise in IP Theft

Every other week seems to bring out a story of industrial espionage—in aerospace, technology or biopharmaceuticals. A Kiplinger news story in January of this year noted that cyber-thieves are increasingly working behind the scenes to sell and deliver American and European company secrets to overseas competitors.

In the meantime, there has been a rise in overseas outsourcing from pharmaceutical and biotechnology companies looking to reduce expenses. While some of this is in manufacturing, the majority of outsourcing so far has been in preclinical research and development and in clinical trials, providing non-company personnel direct access to a firm's developing intellectual property.

At the end of 2007, the Department of Commerce's International Trade Administration released its summary of countries with whom it is struggling to advance US intellectual property protections. While China may come as no surprise, few executives are aware of the second-class status of their intellectual property in India, Israel, the Philippines, Thailand and Mexico.

While these reports set the stage on the international scene, what is also on the rise is trade secret theft inside a company. Recent lawsuits involving former executives of medical device firm Kinetic Concepts, aerospace giant Boeing and tech firms Quantum3D and SAP should give you pause for thought.

Joel Brenner, national counterintelligence executive in the Office of the Director of US National Intelligence, discussed a great shift toward increasing espionage reliance on private sector employees during a recent speech. His main point: employees of US and European companies can make quick cash by selling electronically-stored documents to overseas

organizations simply through email and web-based payments. Given the economic turmoil around the world, how certain are you that your trade secrets and new IP are safe?

Gone are the days of dark street corners and cash-laden briefcases; today, IP theft occurs with the click of an email and an online bank deposit—it's far safer, far faster and far more difficult to detect.

So what to do?

Decide What to Protect

One of the first items we ask our clients for is a list of the types of information they consider critical to business operations. To date, no one has even a simple list typed on a single sheet of paper. If you do not know what you need to keep safe, how do you expect to protect it?

The first step is to identify the information you need to protect. Consider prioritizing your efforts on truly proprietary information such as unique processes, formulations, home-grown software, customer details, and so on.

The simplest way is to ask your colleagues, "What do we have that gives us a competitive advantage (or will allow us to have a competitive advantage, in the case of new products) that no one outside of our company knows about?"

When you've identified this information, it is time to explore where that information exists. And you may be in for a surprise.

Segregate SOP Information

In an ideal world, no one individual would be able to put together the puzzle pieces of your intellectual property by themselves. Unfortunately, in their zeal to detail out procedures, companies inadvertently place step-by-step instructions to recreating intellectual property in their standard operating procedures (SOPs).

In our consulting engagements, we have seen this most often in SOPs that tackle formulations, mixing, assembly (for medical devices), and even in-process or post-assembly quality testing.

Conduct a review of your SOPs that relate in some way to your intellectual property. Look for detailed Step 1, Step 2, etc. processes that would give a knowledgeable person enough to duplicate your product.

Revise your SOPs to eliminate any trade secret-revealing step-by-step details, making sure to still capture the process and its regulatory and quality requirements. This is a fine line to walk, but a necessary one.

If you are using a contract manufacturer (CMO)—especially for new product pilot production or clinicals—this review (and revisions to SOPs) is absolutely essential.

You may also want to take this review one step further and look at the CMO’s internal SOPs related to production of your product. Their SOPs may very well spell out your IP in step-by-step fashion.

Communicate to Personnel

If your personnel do not know that particular information is confidential, they may not know not to share it—or at least to ask permission before sharing it.

This does not mean you spell out the particulars of your trade secrets, but rather you note that (in the case of a drug) the formulation is considered highly confidential and will only be shared with certain individuals. We recommend you also clarify that information supporting the creation and testing of the formulation may be confidential as well.

Work with your computer department to ensure that access to the information is restricted and monitored. Simply restricting access is like expecting a locked door to prevent burglaries. Some level of monitoring is necessary to deter a would-be thief. Tell personnel that the company has monitoring in place, just as a burglar alarm company places a “protected by” sign out in front of a building.

Final Thoughts

Deciding what to protect, communicating its importance to personnel and ensuring your SOPs are not inadvertently providing step-by-step trade secrets recipes are only a few of the tactics to master when it comes to saving your intellectual property.

Fundamental to all of this is recognizing that the greatest threat is not without, but within.

Ignoring the realities of internal risks ignores reality: employees do not work for you for their lifetime; contractors come and go; and outsourced partners grow stale. In the end, money is always more tempting than any corporate mission statement.

Are you ready?

About the Author

John Avellanet is a former *Fortune 50* subsidiary C-level medical device and biotechnology executive where he created, developed and ran his firm’s Records Management and IT departments, and was accountable for trade secret protection. In 2006, he founded his independent consulting firm, Cerulean Associates LLC (www.ceruleanllc.com) and has since become one of the leading experts on trade secret espionage protection.