

Manufacturing Business Technology

Intellectual property security basics

Some rules of thumb—and some technologies—that protect product information in outsourced environments

By Nancy Bartels

Manufacturing in low-cost countries makes great bottom-line sense. It even may be necessary for corporate survival. But doing so can put a company's most valuable asset—its intellectual property (IP)—at risk. Having operations or partnerships in places where notions of property rights might not yet be fully developed means companies must guard key product designs, processes, and other information more carefully than ever.

"Look at how many products are commoditized because someone has reverse-engineered or made black-market copies," says Jim Brown, a VP at Boston-based **AberdeenGroup**. "Not to mention that we send files back and forth with enough detail that somebody could—in theory, at least—plug the information into an NC [numerical control] machine and produce the part. People are able to knock off extremely complex products."

But it's not just product designs that are at risk. "IP is more than patents and copyrights," says Steve Ganster, managing director at the Shanghai-based consulting firm **Technomic Asia**, and coauthor of *The China-Ready Company*. "It's customer access, market knowledge, and process knowledge. When someone else manufactures products for you, it's exposing the process. It may not be a copyrighted or patented process—just years of experience. In many companies, that's the real advantage." And how do most companies today secure intellectual property?

"Today the most common strategy is the trusted-entry approach," says Mike Morel, director for manufacturing solutions, **Adobe Systems**. "That works for the first tier of trusted partners, but as you move farther and farther away from the system of record, it gets tougher and tougher to manage. Can you trust your partner's partners' partners? You lose control of the document."

If technology makes it easier to steal intellectual property, it's a safe bet that technology will be used to secure it as well. And vendors, especially in the areas of product data management, are offering innovations that reflect the heightened security concerns that are part and parcel of globalization.

Defensive due diligence

Before speaking about new technology, it's good to have a few basic principles to live by when it comes to information security.

It begins with the basic question of whether to outsource at all. Companies need to evaluate the risk/reward equation, says AberdeenGroup's Brown. Are the risks of sharing IP with an outsourcing partner outweighed by the benefits? Researchers at Needham, Mass.-based Tower Group say risk-management measures to secure IP can cost 15 percent to nearly 20 percent of the savings gained from going offshore.

Manufacturers should ask themselves, "What's the motivation to go? What's the urgency?" says Ganster.

Having decided to go ahead, the knotty issue of the exact nature of the relationship with the overseas partner must be addressed. Will the partner be involved in codevelopment? If so, who owns the results? Who else does the supplier work for? Can its work with competitors be limited? Will it manufacture entire products, or just parts? How much of the work will it outsource? These questions need to be answered before moving ahead.

Ganster recommends registering patents and trademarks in the outsourcing partner's country and having the relevant parties sign strong non-disclosure and noncompete agreements. "These agreements may not be enforceable," he points out, but doing so can 'send a message'."

Building relationships with the local business and law enforcement community also is important, adds Ganster. "There is a concept the Chinese call 'guanxi' [pronounced gwan-she]. It means relationships or connections, but it's more than that."

Be stingy

Once a company decides to outsource, it's best to share as little information as possible, says Ganster. Many companies outsource only peripheral items, keeping all core IP at home.

A second strategy is to break up the IP—not giving all of it to any one supplier. "Give contractors access to part of the picture," says Brown. "Let a contract manufacturer see one part of the overall design, but not the whole thing."

Give suppliers only the information needed to do the job. "At the bid point, if five possible suppliers are given 3D CAD drawings or hi-fi representations in a neutral format, anyone of them can produce that part," says Brown. "But all that information isn't needed. Share just what is needed to make the bid."

Once a manufacturer has picked its partners, it can look to technology to further ensure security. Product life-cycle management (PLM); enterprise rights management (ERM); CAD, and security vendors all offer solutions.

Systems use multiple approaches to security: managing access, authentication and authorization of users, version control, encryption, auditing and tracking; and controlling the level of detail conveyed in CAD files.

A balancing act

How can the right balance between openness and risk management be attained?

Proficiency's Collaboration Gateway solution addresses this problem at the data level, says John Alpine, CTO of the design collaboration software vendor. IP owners designate what parts of an assembly should be shared in a detailed, feature-based format; and which parts are shared as geometry "lumps"—that is, without internal details.

"There's a template unique to each partner," explains Alpine. The templates specify the level of detail in the files each partner gets. "It's like turning a knob. It's a way of saying how much data should flow through the pipe."

PLM vendors offer similar options. For example, **UGS' JT** technology is a data format commonly allowing aerospace and automotive design information exchange at varying levels of detail. The system can send complete model information—including geometry, attributes, and product manufacturing information—or little more than facet data, a way of approximating the surfaces of a solid model with triangles.

Other vendors let IP owners control information access and track all sorts of electronic documents—including text files, spreadsheets, and e-mail.

"The design collaboration environment has three layers," says Adobe's Morel. "The first two are the design and visualization layers that work around native files. Underneath that is the document-based collaboration environment. It includes communication between engineers and the 'extended engineering' community—tech support, marketing, quality control, and so forth. CAD files aren't needed there."

Adobe delivers security by means of its Intelligent Document Platform. Adobe LiveCycle Policy Server wraps content objects inside configurable logic that allows users to attach a set of rights specific to that particular document.

The set of rights begins with authentication, Morel adds. Then, once the system determines it is dealing with an authorized user, it also controls what can be done with the document.

"I can specify what kind of rights you will have with that package—to read, write, copy, or forward it," says Morel. "I also can set time limits, allowing access for 'x' number of days, but after that it can't be opened or forwarded."

Capabilities continue even if the user takes the document off-line. "As creator, you can set up a 'lease.' The document can go off-line for a certain period of time, but when the lease ends, the user has to reauthenticate," says Morel. Forcing the user to put the document back online to access it also allows the originator to track its use on an ongoing basis.

Recently, Adobe and UGS enabled manufacturers using UGS' JT data format for 3D models to publish them as Adobe PDF files, thus establishing control at both the data and document level.

About the mail

Not all collaboration takes place by means of CAD or PDF files. It's no secret that e-mail is the collaboration technology of the century, and is great for semi-formal communication.

ERM vendor **Authentica's** Active Rights Management platform combines document security and e-mail protection. Its Secure Mail module has the same kind of policy-setting capability as Adobe Policy Server—for access control, copy and forwarding privileges, and time limits—for e-mail, including attachments. Secure Mail works with both Microsoft Outlook and Lotus Notes, and also can be used with wireless tools, such as the BlackBerry.

IP protection must go beyond software. Companies should consider practices such as a "clean desk" policy, where nothing is left in sight overnight; strict lockdown of servers, desktops, laptops, and removable storage; and taking charge of the computer infrastructure of the offshore company. At the very least, they should exercise the same level of computer security at offshore facilities as they do at home.

In the end, there is no 100-percent security guarantee when intellectual property leaves the four walls of the enterprise. "All you're trying to do is increase the barriers," warns Brown. "There is no silver bullet."

[Privacy Policy](#)

© 2005 Reed Business Information, a division of Reed Elsevier Inc.
All rights reserved.

The URL of this page is: http://www.mbtmag.com/current_issues/2005/dec/secwire1.asp