

January 2009

Collaboration without compromise: How to protect intellectual property as it traverses global supply chains

By Ann Avery

In manufacturing today, the walls have come down. The need to collaborate effectively with partners and suppliers has pushed organizational boundaries beyond the four walls and across the information technology (IT) firewall.

In automotive and process environments, the semi-conductor world, and many other

manufacturing sectors, collaboration is increasingly critical to building a competitive advantage in the 21st century.

“As we look at the mega trends in the marketplace today—increasing complexity around the supply chain, the pressure to get more products out more quickly, and the need for worldwide partnerships and global service

delivery—they all drive toward expanding collaboration,” says Mike Morel, director of manufacturing solutions at Adobe Systems, a premier supplier of technology that facilitates electronic collaboration.

But while this collaborative business model is delivering enormous benefits for manufacturers, it also presents serious threats to intellectual property (IP). These threats are not always readily apparent, but they are real—and they have the potential to destroy a company’s competitive position.

The best way of thwarting these insidious IP threats is using technology to embed automatic digital rights management (DRM) capabilities into your collaborative business processes. Fortunately, the technology is available to develop these capabilities fairly easily, and inexpensively.

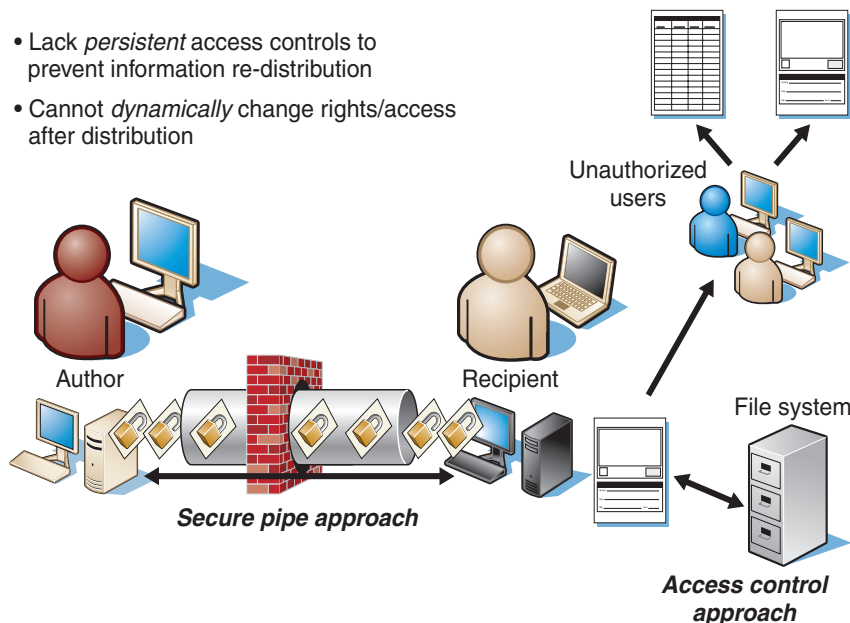
“As manufacturers share data with partners around the world, they are taking very real risks,” says Morel. “Not a week goes by without a headline about the threat of IP loss. It’s critical to understand that a strong DRM system is an essential component of any successful collaborative strategy.”

Collaboration survey highlights the very real risks to IP

The problems associated with protecting IP were highlighted in a recent AMR Research survey of 150 global manufacturers commissioned by Adobe. Survey responses indicated that almost 50 percent of companies have

Shortcomings of current information assurance approaches

- Lack *persistent* access controls to prevent information re-distribution
- Cannot *dynamically* change rights/access after distribution



Falling short: Many companies have adopted information control policies that don't adequately protect intellectual property.

Better collaboration requires information delivery to anyone, anywhere

700 million
PCs and devices

Source: NPD December 2005

Widely connected: Adobe technology is readily available, and easy to connect to any communications environment.

formal, automated processes for collaborating with partners. And while most companies attempt to protect the information they exchange with suppliers, the survey revealed that more than 60 percent of IP security programs are managed manually. Morel says these numbers indicate that a large percentage of companies have collaborative processes that are unmanaged, uncontrolled, and unsecured.

“Even though companies have invested huge amounts of money in applications to help secure IP, significant collaboration still happens outside of these applications,” says Morel. “It’s imperative that manufacturers change the ways they collaborate—both to enhance the collaboration itself and to minimize risk.”

Re-tooling collaboration strategies for the 21st century

As manufacturers examine how to make collaborative efforts more effective and secure, the first step should be taking a fresh look at who is participating in these processes.

“Most organizations have focused on collaboration in the context of expert to expert. But our experience demonstrates that it’s vital to look at a broader audience across the complete manufacturing ecosystem,” says Morel.

Making sure that everyone is involved is a challenge, especially when collaborating with

smaller partners. Organizations without a lot of technology or applications in place can be difficult to include, but they must be part of the process, says Morel. And businesses can no longer assume a certain level of education, application, installed base, or even language as they collaborate across supplier and partner networks.

“To foster meaningful collaboration across this broader audience, you need to communicate in a richer way with more information than ever before,” Morel says. “At the same time, information packages need to be tailored to be easy to use and cause minimal process disruption. And obviously, if you’re delivering and sharing more robust information, then it’s essential to protect, manage, and control that information everywhere it goes.”

Critical issues in designing effective DRM

In the process of defining needs and policies for a DRM solution, Morel advises manufacturers to take a close look at some of the collaboration processes that are especially prone to IP risk such as:

- Design collaboration
- Engineering Change Order (ECO) management
- RFx/supplier collaboration
- Work instructions/process sheets
- Field service management

“Product designs are typically a prime target [for IP theft],” says Morel. “However, any communications regarding changes, the links between engineering and manufacturing, and all of the documentation necessary to manage a field service delivery process can be very

Adobe DRM helps manufacturing companies collaborate

Adobe supports high performing manufacturers by:

- Enabling people to engage with ideas and information **anywhere**
- **Leveraging existing applications** to deliver the right information, to the right people, at the right time
- Ensuring that intellectual property is **managed and controlled** everywhere it goes

- Employees
- Partners
- Customers

- Legacy applications
- ERP
- SCM
- CRM
- PDM

- Product lifecycle management
- Supply chain management
- Enterprise resource planning
- Customer relationship management

Source: NPD December 2005

A complete solution: Adobe DRM helps manufacturing companies collaborate securely.

sensitive and vital to a company's ability to compete," he notes.

"Determining exactly what you need to protect is the critical first step in developing an effective DRM system because it drives the rest of the solution design," says Jeff Legters, solution delivery manager for Cardinal Solutions.

Cardinal Solutions is an IT solutions provider and systems integrator with extensive experience implementing DRM systems. Legters says it can take weeks or months to implement a DRM solution, depending on the complexity of the requirements and what existing systems are already in place.

It's important to understand that you don't always need to start from scratch in terms of designing a secure solution, says Legters.

"Adobe LiveCycle Rights Management ES software, for example, is designed to layer additional digital rights management on top of the rights management in existing application," says Legters. "A company may already have a well documented security model for certain internal materials, and we could map those existing requirements to extend the DRM solution outside of the enterprise."

Must-have DRM features

In the world of high-performance manufacturing, employees, partners, and customers must be able to engage with ideas and information anywhere, says Morel.

"Whatever legacy application or process is involved—product life-cycle management, supply chain management, ERP, or CRM, for example—companies need to get information out of these applications and deliver it in a safe way to a broad set of collaborative partners," Says Morel.

Morel also notes that many companies who believe they are protecting IP are not doing an adequate job because they are relying solely on what he calls "the trusted entry approach." This involves the use of passwords, encryption, and the like to ensure that only certain people can get access to IP. "The problem is that once the information passes through the firewall, all protection is lost," Morel says. "Clearly, this is a major issue when you're talking about collaboration across the globe."

Dangerous leaks plugged by Adobe

How insidious are threats to intellectual property? Consider the case of one highly successful electronics manufacturer that was using contract production facilities and collaborating with designers and manufacturers in the U.S. and around the world.

This company learned exactly how ineffective its rights management strategies were when a story about a product it had not yet released appeared in a trade publication.

"Because this information was published a few months before the product was to be released, competitors were able to add some of the same features to their products and diminish the value of the upcoming release," says Todd Burke, Adobe LiveCycle solutions specialists.

"The impact was millions of dollars, and the company determined that someone in its external supply chain had leaked the information."

Adobe worked with this manufacturer to identify requirements for the right DRM solution to address its challenges.

"First, it had to be easy to use," Burke says. "For anyone in the supplier/partner network, there needed to be a path of least resistance for the majority of the documents that they had to open. Second, the solution needed to integrate with the company's existing Documentum content management system. And third, it had to be deployed through an extranet."

In summary, the new solution needed to fit tightly into the company's existing environment.

Adobe LiveCycle Rights Management ES helps companies leverage and extend applications and information that are already in place for comprehensive rights management. This was an ideal solution for the electronics manufacturer's problem.

"The manufacturer used the infrastructure components of the Adobe LiveCycle suite, the API [application programming interface] calls, and their own development team to rapidly put together a solution that enables automated protection and ease of receipt of documents," says Burke.

The internally built solution at the company includes LiveCycle Rights Management ES, Adobe Reader software, and Adobe Acrobat software. "Their LiveCycle Rights Management server is connected to a Documentum environment that feeds the server any documents that need to be protected. The legacy content management system still controls the creation and deployment of those documents," explains Burke.

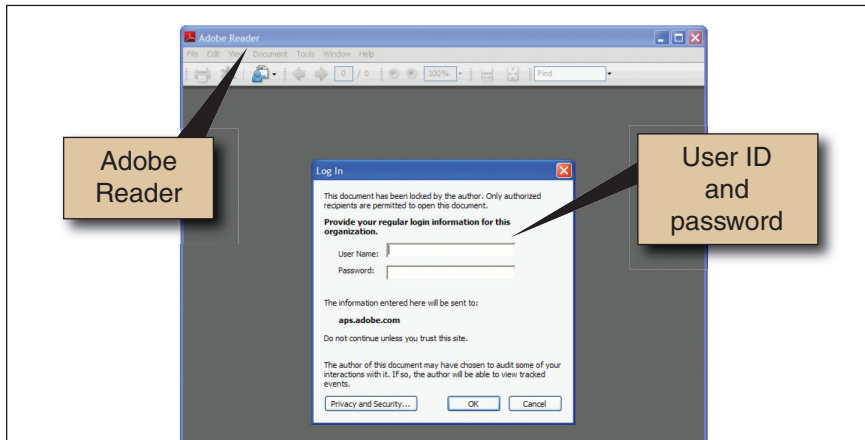
Dramatic improvements with minimal disruption

The experience for the document publisher needed to be as simple as possible, so the protection is automatied. "People posting documents inside Documentum do not need to know anything about applying rights management, they just follow their normal workflow," says Burke.

The minimum technology requirements for people receiving documents are Adobe Reader and an account on the extranet. "Both of these are in place for the majority of the suppliers and partners who deal with this company. So, the new system causes minimum disruption while providing maximum release of protected information," says Burke.

The majority of the company's important IP—such as design documents with

cont'd on next page



Secure collaboration: Adobe solutions have built-in mechanisms for ensuring only authorized users can access information, Adobe solutions have built-in mechanisms for ensuring only authorized users can access information, even as the information travels across the globe.

Legers agrees that access control on a Web site or extranet is not enough in the global environment. “By combining user authentication and permissions identified in policies, advanced DRM systems such as Adobe LiveCycle ES can dictate what access the user has to the document (to view, print, modify, or save, for example) and control some document display options such as watermarks—even beyond the extranet,” he explains.

The ability to change policies after a document is distributed outside the enterprise is among the DRM features commonly leveraged by his customers, says Legters.

“Advanced DRM systems enable a policy-protected document to ‘phone home’ to the server to authenticate the user and verify permissions each time the document is accessed,” says Legters. “Even after the document is distributed, we can affect user access by configuring the policy at the server. The next time the document is accessed, it phones home, and the updated policy is applied. This is also a good way to manage version control because you can take away the rights to access the outdated document, and force access of the current version,” he says.

Other DRM features commonly required by Cardinal Solutions’ customers are automatic expiration of permissions and forensic audit trails that trace not just users but also their specific attempted actions, says Legters.

Defining the most important DRM features for your organization requires a thorough understanding of how various types of information is used—and by whom—across the value chain. “When you understand your company’s

precise needs in terms of IP security, you can then find a DRM solution with the flexibility to map to those needs,” Legters advises.

Morel emphasizes that if the processes for protecting documents are complex, your partners and even your employees will simply not use them. Advanced DRM solutions enable automated protections that have minimal impact on user workflow and the recipient’s desktop.

With an Adobe DRM solution, the basic technical requirements for most information workers to receive fully protected information—leveraging Adobe Acrobat Reader and Flash Player—are often already in place even at less technically sophisticated partner companies.

Says Morel, “When you select a DRM solution, remember that you can secure IP without changing your business processes and without making major investments in new technology. The vital issue is that IP must be protected, managed, and controlled everywhere your information goes.”

Leaks continued

cont'd from previous page

3D components—is contained in documents in Adobe Portable Document Format (PDF). “The recipients receive the documents in PDF, and the company is planning to deploy Microsoft Word and Excel formats down the road,” notes Burke. “Adobe also supports the CATIA format and is working with PTC to support for Pro.E file formats.”

In the past, this company’s PDF documents were released through the extranet with no protection. “Now, however, the end user uses the same process, and workflow runs the same way, but there is one additional step,” explains Burke. “Some of the attributes from the workflow are sent over to the Adobe LiveCycle Rights Management server which uses them to pick the policy and level of encryption. The Adobe server encrypts the document and returns it to the content manager. Finally, the content manager sends the secured PDF to the recipient who opens it in Adobe Reader.

“With the Adobe solution in place, this manufacturer has experienced its longest release cycle with no identifiable leaks,” says Burke. “While they have had very few support issues from their external customers, partners, and suppliers, they have far more sophisticated controls than in the past.”

For more information

Adobe sales: 888-649-2990

Have Adobe contact me

http://www.adobe.com/cfusion/mmform/index.cfm?name=contact_us&sa=manufacturing

Learn more about Adobe’s manufacturing solutions:

<http://www.adobe.com/manufacturing/>

For additional information on Adobe’s DRM solution:

www.adobe.com/manufacturing/drm.html