A False Sense of Proprietary

Abstract: Organizations often resist standards in order to protect their proprietary information and processes. Protecting proprietary information is essential. However, enterprises often have a misplaced idea of what information is truly proprietary to their business. The protection of information has cost associated with it. While it is important to protect intellectual property, it is also important not to protect that which is part of the broad state of the art. Furthermore, some information increases dramatically in value when shared in a collaborative environment. This article explores the concept of a misplaced sense of what is proprietary, the business case for separating proprietary and non-proprietary information, and the value of standardizing the latter.

It's ours… All ours… Protect it All!

It's a natural reaction. Our team works its fingers to the bone on some piece of support software and we want to protect it. After all, it's the safest thing. If we open ourselves up to the prospect of sharing some of our work, there is danger in making a mistake. The mistake can go one of two ways:

1. **The Cat's Out of the Bag** — If information is shared that shouldn't be, the business can be damaged. Competitors can be given a leg up against us. We can see our developments being offered to our customers by someone else at ridiculously low prices. Our competitive edge can be compromised. The potential for disaster is clear.
2. **Mum's the Word** — If information is not shared that could be, what can be the harm? If everything is protected, then all is safe.

So "Mum's the Word" then. With this approach we don't have to think through what could go wrong with sharing the information. "No" is the easy answer and is the knee-jerk reaction of many corporate managers and attorneys because it seems to carry the least potential for disaster.

"Protect it All" has been a common approach in protecting Intellectual Property, but overlooks several aspects of the issue:

1. What is the Cost of Protecting Information?
2. What are the Benefits of Sharing Information?

---

* Larry L. Johnson

3. What is proprietary? Once we decide to share *some* information, how do we decide *what* should be shared and with *whom*?

THE COST OF PROTECTING INFORMATION

Protecting information is not free. There are costs associated with it.

That Which Is Everything Is Nothing: If common commodity information is under the protection of an organization, employees become numb as to what is truly proprietary. It becomes difficult to recognize the difference between proprietary information and blanket "Mum's the Word" protection. Blanket silence can make it extremely difficult to have a conversation in public venues without stepping on proprietary information resulting in difficult or impossible enforcement.

Barring the Doors: Limiting access to information is a necessity in containing and controlling it. If there are too many "leak-points" in an organization, it is impossible to assess leak sources. If one cannot determine the source of a leak, then one cannot assign culpability. Consequently, all deterrents fail. A costly side-effect of limiting access is the interruption in the flow of information among employees. There is danger that information will not be available to the right people in the organization at the right time. Rapid response to the quickly evolving business milieu requires agility which in turn requires timely access to information.

Hire More Attorneys: A good way to protect innovation is through patents and copyrights, recognized by the courts. The downside of patents is that they must be protected. In order to protect the patents, research must be done to find infringements or to assure that there are none. When infringements are found, remedies must be found (often through the courts). All of this incurs expense.

In summary, the more information is protected as proprietary…

- the more workers must be kept ignorant of the information;
- the less communication among workers takes place;
- the more workers fall out of touch with the technological community; and,
- the more money is spent in detecting and prosecuting infringements on intellectual property.

Consequently, it is essential that only "truly proprietary" information is protected.

THE VALUE OF INFORMATION EXCHANGE

Having argued the downside of protecting too much information, we have to ask if there is an upside in sharing information.

We can, of course, start with the converse of the above "downside" points…

- **That Which Is Something Is Useful:** In knowing definitively what is proprietary and what is not, employees can participate freely in the conversations of public forums. This helps the organization keep up to date with developments in technology and with the evolution of their industry's business practices.
- **More Open Doors:** This leads to a more open flow of information within the organization as well, enabling employees to have maximal access to information needed to conduct day-to-day business and to respond rapidly to unexpected situations.
- **Lower Legal and Control Costs:** With less information to protect, fewer resources need to be applied to controlling and protecting information, and defending patents against infringements.
- **Less is More:** A side-effect of loosening control over nonproprietary information is that the control over truly proprietary information is enhanced. Protection resources can be applied in a focused fashion avoiding the dilution introduced by protecting information unnecessarily.

… but the benefits of information sharing go well beyond this. In many circumstances information can actually become more valuable to an organization by being shared in collaborative efforts. These benefits are explored below in three case studies in collaboration.

But before we do that we should look at the separation of proprietary and nonproprietary information.

A False Sense of Proprietary

In their book on collaborative research & development, Allen & Jarman write:

> "The objective of a company's legal staff should be to provide a legal mechanism to enable you to do what you want in collaboration. However, legal and contracts experts in large manufacturing companies have been well educated and trained in the discipline, to protect the companies intellectual property and to err on the side of too much protection. To do this, they have built fortresses of firewalls and layers of protection around products and processes that come in contact with knowledge property deemed key to existence of the business. While companies must continue to protect and defend the real knowledge based jewels that have competitive value, they must also be flexible and clever enough to find ways to peel away the layers which are not critical, so that value adding operations can be performed. Today, companies choosing collaboration are faced with inflexible legal and contracts people who do not understand or believe in collaboration as a viable means of doing business. Aligning these departments as early as possible in the process is very helpful and time saving."[1]

Effective protection of intellectual property, demands that "truly proprietary" information is identified and protected while allowing nonproprietary information to be shared. So how do we "peel away the layers that are not critical"? There is no pat answer. It can be a difficult task, which is why it is not widely done well. "Mum's the Word" seems safe, but of course ignores the cost/benefit issues discussed above, and the greater benefits of information sharing described in the collaborative case studies below.

In order to identify intellectual property, an organization needs to look at its prospectus, formal statements of goals, its business plan, etc. Information that constitutes or directly serves the business case of the organization is that which requires protection.

Part of the difficulty in separating proprietary and nonproprietary information is that there is no sharp boundary, but a continuum of information sensitivity that depends on the business context. The same information may be protected in one context while not others. For example, information might be shared more freely with a partnering organization while protected from competitors. This sharing with partners needs special constraints if the partnering organization might be a competitor in another contract now or in the future.

An organization might develop elements of computing infrastructure that are not available in the commercial marketplace. Some organizations will protect this information while others may openly share it hoping to encourage the appearance of such software in the market.

Proprietary information must be re-assessed periodically. The proprietary nature of information generally decays over time. That which provides a competitive edge at one point, later becomes commodity technology as the technological approach is adopted throughout an industry segment.

Every organization is unique. It is beyond the scope of this article to provide a detailed formula for sieving information into proprietary and nonproprietary categories. The point is that each organization needs to carefully examine their intellectual property portfolios periodically to assure they are not wasting money by protecting common knowledge and to assure that they are reaping the benefits of information sharing and collaboration.

CASE STUDIES IN COLLABORATIVE INFORMATION SHARING

The most compelling case for correctly identifying and protecting intellectual property, and sharing information that is not intellectual property, can be seen in collaborative efforts for process improvements and research & development. The following three case studies from my experiences at Texas Instrument's Defense Systems Group (TI)[2] exemplify the copious benefits that can be accrued in sharing information. The

case studies demonstrate progressive degrees of information sharing and collaboration in Product Data Management (PDM).

Benchmarking: A Case Study in Simple Information Sharing

From 1982 through 1997 I worked for Texas Instrument's Defense Systems (TI), an aerospace company. TI was among the first to deploy a Product Data Management system. In the mid-1980s, there were no viable commercially available PDM products suitable for our use, so we developed our own system at considerable cost. The manager of TI's PDM Systems Group, Travis Mitchell, had an unusually enlightened approach to the proprietary nature of our PDM Technology… *It isn't*. His directive: "There is nothing we do in PDM that cannot be shared, and we will encourage our partners, competitors, and customers to share as well. We are in the business of making missiles, not in the business of Product Data Management."

His position fit perfectly with a "Benchmarking" program that was being instituted by the company in keeping with the most modern trends in business at the time. In benchmarking, a company establishes a relationship with a competitor or a firm in a similar business to compare notes on "the state of the art" in business areas that the companies have in common. Our benchmarking partner was another aerospace company. The principal difference between our companies was that we made missiles and they made airplanes ("targets" in our perspective).

During the benchmarking process we discovered that the differences in our approaches to PDM were not remarkable. We did some things better, while they did other things better; they did some things that we hadn't thought of and vice versa; but all-in-all things were very similar between the two companies.

Up to the point of benchmarking, both companies felt that their PDM systems were a competitive edge and protected their efforts as proprietary information. Why were the fruits of their efforts remarkably similar? On reflection, this is not all that surprising. The engineers were educated in the same schools, using the same text books. Furthermore, many had moved among multiple companies over the course of their careers. Businesses in a particular industrial sector are competing in the same marketplace and have similar requirements. This drives organizations to similar solutions to similar problems.

At the core of the situation… product data management was making the turn from advanced, proprietary practice to commodity technology and business practice, as validated by the emergence of a full and robust commercial market in PDM support systems within a few years. So Travis' position was validated. His call was correct and the company benefited by not suffering the cost of protecting commodity technology and also enjoyed the benefits of sharpening its processes (as did our benchmarking partner).

The benefit of this collaboration was that each company was able to take home plans for improvement in their PDM systems. Each company absorbed the best of each other's system. This enabled them to facilitate their respective business processes, and it is in the business plan and process that real competition takes place. Both companies expend less energy on support systems that are becoming the state of the general art, focusing on their core business plans. And, both companies gain a competitive advantage over companies who expend their energy protecting information that is not in the mainstream of their business case.

Closed Consortium: A Case Study in Aggressive Collaboration

Having enjoyed benefits in their benchmarking projects, TI entered into the first Advanced Technology Program issued by the National Institute of Standards and Technology (NIST), the Rapid Response Manufacturing Consortium (RRM).[3]

The RRM program objective was to shorten time-to-market, improve quality-to-cost, and enhance product reliability. The participants included two competitors in the defense industry and two in the automotive industry. The idea was to share information in order to produce "pre-competitive" technology to which each member of the consortium would have rights to develop further into proprietary technology and business processes.

One of the areas addressed in the RRM was Engineering Data Management. TI, Ford, and Oakridge National Laboratories brought their experiences in PDM to the table. By this time (circa 1994) TI had five different PDM systems in various areas of the organization… some commercial… some home grown. Each of the PDM systems had special features that provided special benefits to the department that deployed it. This precluded eliminating all but one vendor (a simple, but ultimately costly strategy). However, there were many applications that needed to span all PDM data regardless of the system in which they resided.

Ford, TI, and Oakridge in particular shared this problem and teamed together within the consortium to address it. The "Interoperability Services Working Group" (ISWG) was formed to address the problem. In order to integrate disparate systems, the ISWG defined a reference architecture that was suitable for all of the companies. To do this, the consortium members shared their experiences and technical data on the application of PDM systems in the context of their business processes. As an underpinning, the ISWG defined a message-oriented architecture based on the Object Management Group's (OMG)[4] Common Object Request Broker Architecture (CORBA) specification, particularly well suited to the integration of pre-existing systems.

Using this reference architecture, the ISWG defined an operational PDM semantic that was common to all of the systems targeted for integration, using a paradigm of system federation in which systems are integrated without each being aware of the other.

The collaboration resulted in the ability to swap PDM applications among Ford, TI, and Oakridge, regardless of Product Data Management System and regardless of the CORBA vendor/implementation used and solved the problems each company brought to the table. All of this was made possible through the joint efforts of companies in a collaborative framework… sharing information.

Open Standards: A Case Study in Community Collaboration

Just as the Rapid Response Manufacturing Consortium (RRM) was beginning to enjoy the fruits of its collaboration in Product Data Management (PDM), the Object Management Group (OMG) issued a Request for Proposal (RFP) for a "PDM Enablers" specification. RFPs in the OMG are different from those in general industry. To respond to an OMG RFP is to actually do the work… not propose to do it. What is proposed is an actual specification.

The RRM members Ford and TI had the same PDM vendor, Structural Dynamics Research Corporation (SDRC, the Metaphase PDM product provider at the time, eventually became a late joining member of the consortium). Focused on the business requirements of these three members, the ISWG undertook an analysis of the desirability of responding to the standard and came up with the following compelling business cases for going forward:

Vendor's Business Case:

- With a standard semantic and Application Programming Interface (API), the vendor's PDM "engine" can be used with any application written in compliance to the standard.
- Customers are attracted to an open standard that protects their investment should their initial vendor disappear.
- The only thing standardized is the common commodity operations required by all businesses. How it is done is still proprietary. The vendor can differentiate itself in terms of performance, scalability, stability, price, product architecture, etc.
- A variety of client programs can be developed that will work with the vendors own PDM engine, or with the engine of other vendors.
- Developing a standard API in conjunction with major customers reduces risk inherent in developing software. The vendor is reasonably assured that its product will meet its customers' needs and that there will be a market for the product.

End User's Business Case:

- The company can develop applications specific to its business process that will work with any PDM Vendors system.

- The investment in PDM is preserved beyond the failure of vendor.
- Organizations that were writing an integration layer over diverse PDM systems (such as the TI and RRM stories) will have their work reduced dramatically by having much of the capability provided as part of any product compliant with the standard.

Given the analysis, the Rapid Response Manufacturing Consortium (RRM), (through a membership acquired by the NCMS, partnered with Structural Dynamics Research Corporation (SDRC) to submit a proposed specification for the PDM Enablers to the Manufacturing Domain Task Force (MfgDTF)[5] of the Object Management Group. Through an intense collaborative effort, the consortium submitted an Initial Submission through SDRC to the Object Management Group. This submission joined four other initial submissions by IBM and Matrix; Sherpa; Digital Equipment Corporation; and Fujitsu.

The MfgDTF evaluated the submissions, provided their comments, and suggested that the submitters come together to form a single joint submission team. The submitters agreed to do so and the RRM was asked to chair the Joint PDM Submission Team (JPDM). This broadened the collaboration further. The result was an extremely intense collaboration wherein 2-½ day face-to-face workshops were held once a month, telephone conferences once a week, and a constant stream of email.

The fruit of the collaboration was the PDM Enablers Specification that successfully met the requirements of each of the member companies of the RRM as well as many other companies. This reduced the costs of infrastructure and allowed each company to focus on their direct business case. The broad collaboration possible through an open standards organization such as the Object Management Group enabled the standardization of commodity aspects of product data management while preserving the intellectual property of the firms implementing the mechanics of the generic capabilities.

SUMMARY

Protecting information unnecessarily …

- dilutes and weakens the protection of truly proprietary information,
- impedes information flow within the organization,
- impedes information flow into an organization from the community at large, and
- increases the cost associated with information protection.

Organizations need to assess their proprietary information portfolios to assure they are not protecting information that:

- does not serve the direct business case,
- is stale information that no longer requires protection, or

- is commodity information.

Organizations need to look for collaborative opportunities in which they can

- share the costs of pre-competitive development,
- co-develop support software with vendors, customers, and competitors that address commodity needs, enabling the organization to focus on its core competitive business practices.

Notes

[1] Allen, Gene, and Jarman, Rick, Collaborative R&D, Manufacturing's New Tool, Wiley, May 1999

[2] Texas Instruments Defense Systems Group is now Raytheon Systems Company.

[3] The RRM was a $65M Advanced Technology Program (ATP) issued by the National Institute of Standards and Technology (NIST). It was established as a five-year collaboration (1993-97) involving four manufacturing companies – Ford Motor Company, General Motors, Raytheon Systems Company (formally Texas Instruments Defense Systems Group), and United Technologies Corporation/Pratt & Whitney; a National Laboratory – Lockheed Martin Energy Systems (Oak Ridge Y-12); and six software development companies – the MacNeal-Schwendler Corporation (Aries Technology was the initial participant and acquired by MSC in 1993), Cimplex, Concentra (previously ICAD and now Knowledge Technology International), Spatial Technology, and Teknowledge (previously Cimflex Teknowledge). The program was administrated by the National Center for Manufacturing Science (NCMS).

[4] The Object Management Group (OMG) is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications. Its membership includes virtually every large company in the computer industry, and hundreds of smaller ones. Most of the companies that shape enterprise and Internet computing today are represented on its Board of Directors. The OMG now includes over 500 members, including: (1) Platform-oriented Software Vendors providing support for Model Driven Architecture, CORBA Object Request Brokers and other OMG middleware support and modeling services; (2) Application-oriented Software Vendors who offer Model Driven Architecture based solutions to wide varieties of business problems; and (3) End User Companies who participate in partnerships with vendors to define the requirements and roadmaps of the standards to be supplied by the Software Vendors. More can be found at http://www.omg.org/gettingstarted.

[5] The Manufacturing Domain Task Force (MfgDTF) later became the Manufacturing and Industrial Systems Task Force (ManTIS). See http://mantis.omg.org/.