Aberdeen Group

Send to a Friend

Protecting Product Intellectual Property Benchmark Report

Safeguarding Design IP in a Global Market

November 2006

— Underwritten, in Part, by —

Adobe

agile™

Linx/AS™ Envision PLM

PINION SOFTWARE

RADIANCE the software that delivers

Executive Summary

Issue at Hand

The intellectual property (IP) contained in products and product designs is at risk, along with the revenue potential and corporate know-how they represent. Over two thirds of companies surveyed by Aberdeen Group, in fact, indicate that the threat to their product IP has increased over the last two years. Almost one quarter of these companies say it has increased "significantly." A large part of the increased threat is due to globalization of markets. Ironically, the same approaches that are required to enable distributed design and manufacturing networks – in particular more complete product definition and information sharing – are key contributors to IP risk. As global operations become the norm, Aberdeen benchmarks indicate that the largest concern, by far, in global design is protecting IP.

Key Business Value Findings

The threat to product IP is real and tangible. Benchmarked companies report lost market share, lost product sales, product commoditization, and reduced margins in addition to other consequences. In response to these threats, most companies are placing significant focus on safeguarding IP. Over two thirds of manufacturers are actively focused on product IP protection, and almost one third view it as a "top five" priority for their business. Given the potential implications to revenue – both for today's products and tomorrow's – it is not surprising to see the increased attention.

As a result, many companies are developing multi-faceted IP protection approaches that include:

- Legal strategies to protect IP from being copied by others, as well as protecting against infringement claims from competitors
- Business processes that optimize the amount of product information shared with partners by balancing increased innovation and decreased time to market with the associated IP risk
- Technology solutions to protect product information within the firewall and IP shared outside of the firewall with partners

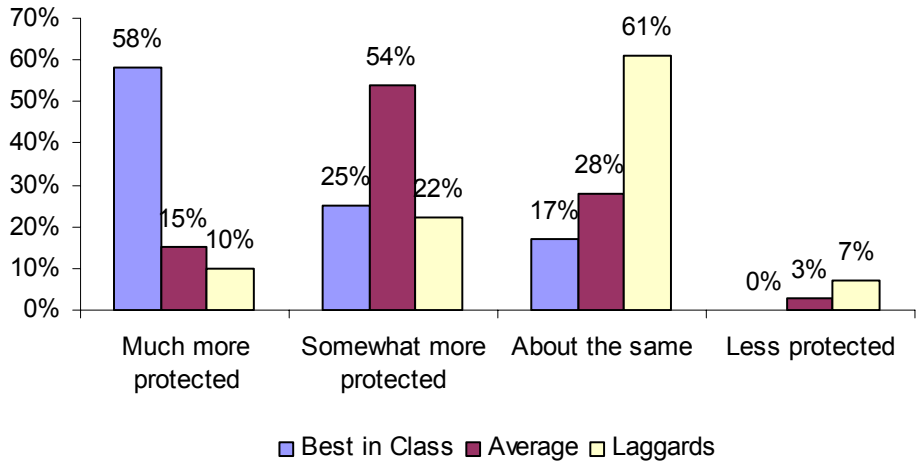
Implications & Analysis

Benchmarks indicate that the steps best in class companies are taking to protect their intellectual property are providing increased levels of protection. These top performers, in fact, are over five times more likely to report significant gains in IP protection than the poorest performers, the laggards (Figure 1). The actions taken consist of business process, organizational, and technical approaches directed at preventing the unintended disclosure of IP as well as providing legal recourse should company IP be abused or a competitor attempt to claim IP infringement against the company.

Leading approaches include:

- Making a senior manager or executive responsible for protecting IP
- Formalizing IP processes and integrating them into new product development
- Measuring IP protection more frequently
- Adopting coordinated or integrated technology strategies to protect IP

Figure 1: Two-Year Trend of Product IP Protection



Source: Aberdeen *Group*, November 2006

Recommendations for Action

To protect their investment in product IP, companies should evaluate their product innovation, product development, and engineering processes to ensure that they effectively:

- Adopt "IP friendly" approaches to collaboration including sharing only the amount of design data required by partners to accomplish their tasks
- Ensure that research and development (R&D) discoveries are captured, evaluated from a business perspective, and safeguarded by executing the appropriate protection (i.e., patents, trademarks, trade secrets, defensive publishing)
- Protect product data, including implementing secure product data management (PDM) and enhanced IT security solutions to safeguard product data within the firewall and digital rights management (DRM) to protect product IP "in the wild" when designs are shared with others outside of the corporate firewall

Table of Contents

Figures

Tables

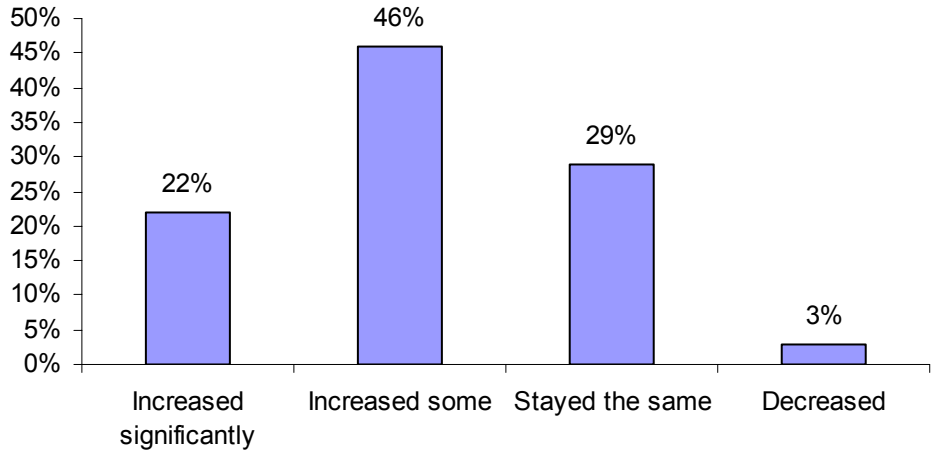
Chapter One:
Issue at Hand

Key Takeaways

- The risk to product IP has increased significantly over the last two years.
- The majority of manufacturing companies today are operating in global markets, putting product IP at exceptional risk of being copied and compromising a company's competitive advantage.
- Despite the widespread recognition of this challenge, common approaches to global design and manufacturing are actually making the problem worse.
- Protecting product IP is as much about protecting tomorrow's products as it is today's, by protecting company know-how in addition to current product offerings.

Benchmark responses clearly show that the risk to companies' product IP has grown significantly over the last two years (Figure 2). Over two thirds of companies indicate that the threat to their product IP – and, therefore, the threat to their profitability – has grown. Almost one quarter of these companies, in fact, say the threat has increased "significantly." An insignificant number, only 3%, indicate that the threat has decreased. Clearly manufacturers are facing a crisis in regards to safeguarding the fruits of their product innovation and R&D investments.

Figure 2: Two-Year Trend of Product IP Threat



Source: Aberdeen *Group*, November 2006

Globalization and IP Protection

A large part of the increased threat is due to globalization of markets, which is a growing concern. Aberdeen's *Product Innovation Agenda* and *Global Product Design Benchmark Reports* from late 2005 report a trend towards globalization. Specifically:

- 59% of companies had a global design strategy in place.
- 44% of manufacturers indicated they were assembling teams across geographies to pursue global design; for discrete manufacturers the percentage rises to 53%.
- 25% of manufacturers were already outsourcing design processes.

Respondents to the current benchmark indicate that the majority of companies are operating as a part of global design networks and global supply chains (Table 1).

Table 1: Participation in Global Markets by Function

Functional Area	% Executing Globally
Design	66%
Procure	53%
Manufacture	62%
Market	65%
Sell	53%

Source: Aberdeen *Group*, November 2006

The impact of globalization on IP protection is significant. Aberdeen's *Global Product Design Benchmark Report* indicates that a full 63% of manufacturers consider protecting intellectual property (IP) as one of their top challenges in global design, representing the largest challenge reported in that benchmark. Many regions in the world, including some of the fastest growing markets such as China, do not operate under the same conventions for protecting intellectual property. At a minimum, the impact is on developing legal protections for patents across multiple countries and languages. At the extreme, the impact is cultural disregard for IP rights and an inability to gain reasonable recourse for IP violations. Therefore, it is incumbent on the owner of the proprietary knowledge to protect it in multiple ways.

Case Study

"To protect intellectual property our patent attorney advised us 'For China, don't waste your time'."

Engineering Firm

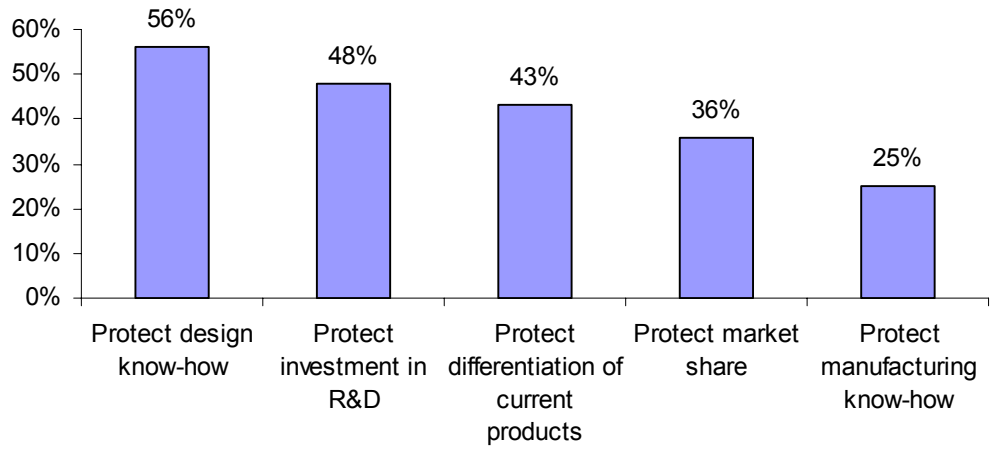
Ironically, the same approaches that are required to enable distributed design and manufacturing networks – in particular more complete product definition and information sharing – are key contributors to IP risk. Despite the widespread recognition of this challenge, common approaches to global design and manufacturing are actually making the problem worse. Leading companies, however, are adopting best practices that allow them

to continue to support their global environments without needlessly placing their IP at risk.

The Importance of Product IP Protection

One could argue that current fast-paced markets and increased ability to "reverse engineer" products has made protecting product designs less important. The challenge, however, is that the modern design incorporates more than just the resulting product. Product definitions also incorporate, and have the potential to betray, a significant amount of company knowledge. In fact, the most prevalent driver for the current focus on IP protection is safeguarding design know-how (Figure 3). Keeping designs secure is important to protecting current products, but also to defending the profitability of future products by securing design knowledge.

Figure 3: Strategic Drivers for Protecting Product IP



Source: Aberdeen *Group*, November 2006

More significant, perhaps, is that benchmarks indicate that companies have experienced real, tangible losses due to compromised IP (Figure 4).

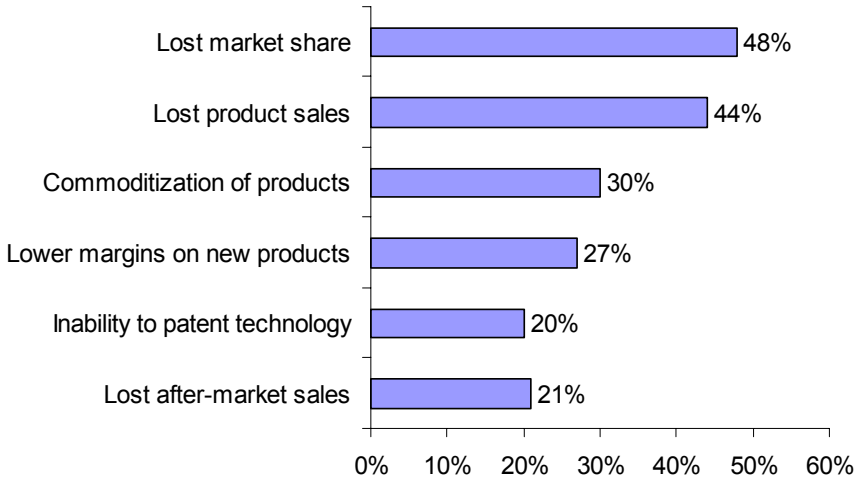
Case Study

"Our component supplier went into business for themselves, making replacement parts for our products."

Industrial Equipment

These losses directly impact a company's top line. Almost one half of the companies benchmarked indicate negative effects on sales volume due to IP loss, including lost market share and product sales. In addition, companies report profitability-related repercussions including having their products viewed as commodities. One interesting finding is the potential impact on after-markets sales. If third parties are able to make precise replacement parts, then service part sales can be diminished. This can have a major impact on profitability because many companies enjoy significantly higher margins on after-market sales than on initial product sales, and most of them cannot afford for these profits to be compromised.

Figure 4: Consequences of Compromised Product IP



Source: Aberdeen *Group*, November 2006

In response to these market conditions, or pressures, companies have been investing in improving their IP protection. To better understand the approaches that companies are taking to protect product IP, benchmark respondents were surveyed on the actions they are taking as well as the organizational capabilities and technology enablers they have put in place to achieve their goal of protecting this important company asset. Using Aberdeen's "PACE" (see PACE Key at right) and "Competitive Framework" (see Competitive Framework key below) methodologies, survey respondents were classified into several tiers of performance to determine which approaches are more prevalent in companies that are leading the pack in protecting their product IP. The following chapters highlight the results of this analysis, including the approaches companies are taking and the results they are achieving.

PACE Key — For more detailed description see Appendix A

Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows:

Pressures **—** external forces that impact an organization's market position, competitiveness, or business operations

Actions **—** the strategic approaches that an organization takes in response to industry pressures

Capabilities **—** the business process competencies required to execute corporate strategy

Enablers — the key functionality of technology solutions required to support the organization's enabling business practices

Competitive Framework Key

The Aberdeen Competitive Framework defines enterprises as falling into one of the three following levels of practices and performance:

Laggards (30%) —practices that are significantly behind the average of the industry

Industry norm (50%) —practices that represent the average or norm

Best in class (20%) —practices that are the best currently being employed and significantly superior to the industry norm

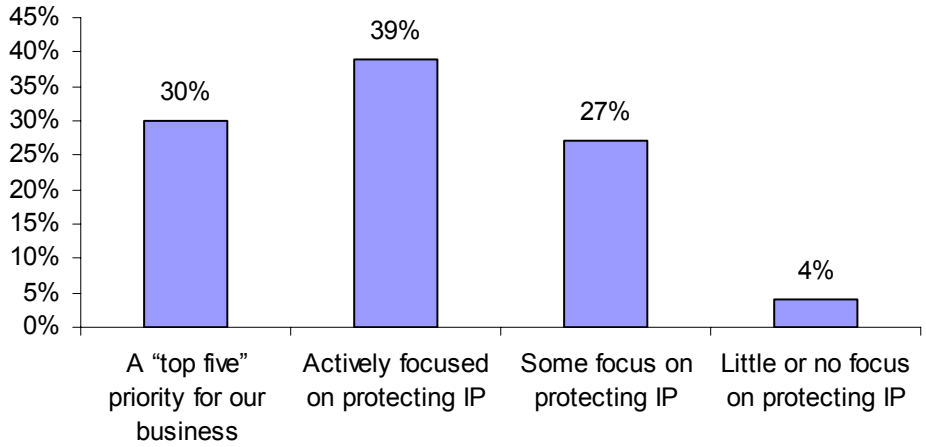
Chapter Two:
Key Business Value Findings

Key Takeaways

- Leading companies are actively focusing on protecting product IP and implementing multi-faceted IP protection plans.
- Companies are adopting "IP friendly" approaches to collaboration that balance the need to document and communicate products for global manufacturing and design with the need for IP protection.
- Organizations are focusing on better documenting the discovery of IP and enabling legal protection such as patents, trademarks, trade secrets, and defensive publishing.
- Businesses are enhancing their ability to protect product data and ensure access by only selected employees and partners.

In response to intellectual property threats, companies are beginning to place significant emphasis on safeguarding IP. Over two thirds of manufacturers are actively focused on product IP protection, and almost one third view it as a "top five" priority for their business (Figure 5). Given the potential implications to revenue – both for today's products and tomorrow's – it is not surprising to see the increased attention. Protecting product IP is becoming an increasingly strategic business requirement as business continues to globalize.

Figure 5: Corporate Priority on Protecting Product IP



Source: Aberdeen *Group*, November 2006

The Product IP Paradox: Enabling Global Business, Jeopardizing IP

Case Study

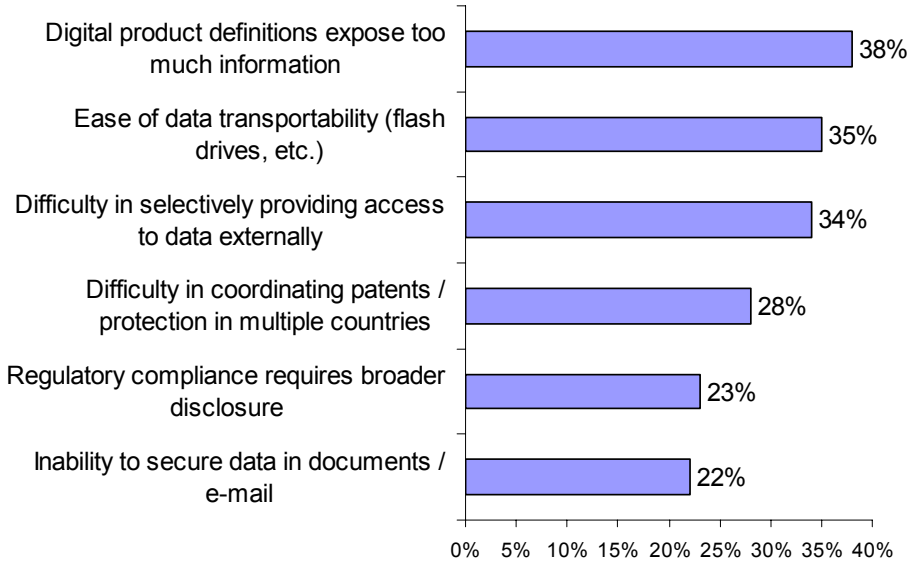
"The concern goes up to the highest level of the company; we put a senior VP in charge of protecting IP"

Industrial Equipment

By its very nature, global business requires more frequent, more interactive, and more detailed communication about products. For a product to be produced in a plant that might be half way around the globe, the designs must be more fully defined and lack ambiguity. Without the informal interaction between designers and manufacturers who work close by, much more manufacturing knowledge must be included in the designs. Product knowledge that previously went unrecorded is now being formally defined and communicated to enable global business.

The number one challenge identified by survey respondents, selected by more than one third of respondents, is that digital product definitions expose too much information (Figure 6). Computer-aided design (CAD) files, for example, may now include materials of construction, design equations, engineering constraints, design macros, or manufacturing information such as precise measurements, computer-aided manufacturing (CAM) instructions, and geometric dimensioning and tolerancing (GD&T). A CAD file typically stores the final product, but also provides insight into the "design intent" or the engineering knowledge used to develop it in the first place. This challenge is directly related to the top business driver reported for IP protection – protecting design know-how.

Figure 6: Challenges to Protecting Product IP



Source: Aberdeen *Group*, November 2006

This is particularly true for products that are being designed in multiple locations concurrently. Design approaches that include digital mockups and automated analysis functions adopted to enable parallel design often depend on more fully defined designs. The chal-

lenges that companies face in safeguarding product IP, in many cases, are a direct consequence of global business.

Other concerns – such as ease of data transportability (reported by 35%) and inability to secure data in documents and e-mail (reported by 22%) – point to the fact that design information is much easier to share than in the past. Large CAD files can now be downloaded onto a flash drive or a portable hard drive, and information can now be readily transmitted electronically via e-mail attachments or FTP. Centralized product data, identified as a key enabler of meeting product innovation and product development targets in the *Product Innovation Agenda Benchmark Report*, is identified by over one third of responding companies as a challenge because of difficulties in providing selective access to that information. The technology enablers that have been developed to help companies collaborate have also contributed to heightened risk to IP.

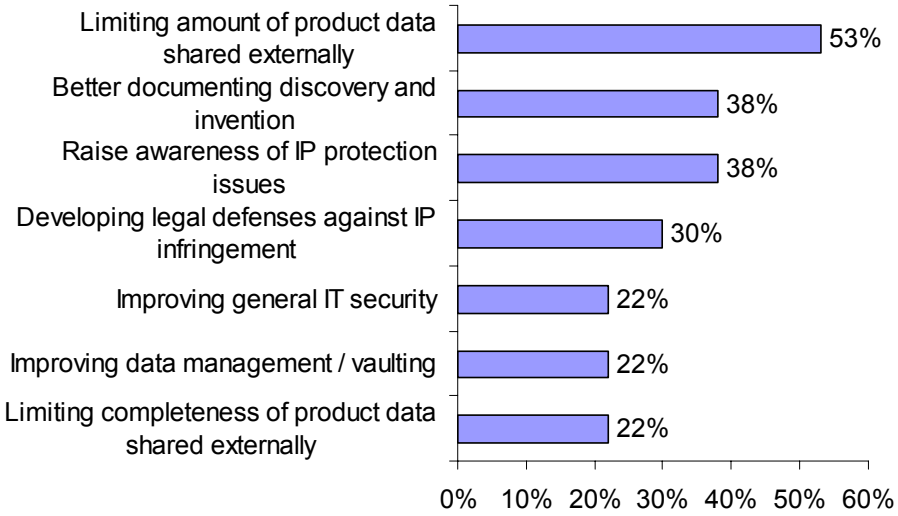
Given the reality of today's market, companies must find the balance between enabling the sharing of product information and protecting IP by developing IP protection strategies that address the realities of their business today.

A Framework for Action to Protect IP

As a result of their strategies to protect IP, companies are taking actions (Figure 7) including new or expanded legal, business process, and technology approaches. Each of these approaches has its merits, but each also has its shortcomings.

- ***Legal protection*** can be used as a deterrent to IP infringement and can provide the rightful inventor of the IP with recourse should companies breach the protection of patents or trademarks. Over one third of the respondents, in fact, are taking action to better document the discovery of IP and inventions. Almost one third are also developing legal defenses against IP infringement. These approaches can be costly, however. In addition, they may not be effective in all markets and require companies to monitor and react to competitive actions that infringe on IP rights.
- ***Business processes*** can limit the amount of IP that is shared with partners outside of the corporate firewall. Approaches such as modularizing design to ensure that only the primary company can see the "big picture" can be utilized to protect the overall product. But this approach does not fully protect against IP infringement from inside sources and may limit innovation because partners do not have the full context of what they are working on.
- ***Technology*** can be used to reduce the likelihood of unintended IP sharing and enable the distribution of more protected product information. Almost one quarter of the companies surveyed report business initiatives to improve data management, vaulting, and overall IT security. These solutions can provide a strong defense, but, like many of the business processes, do not provide protection against inside IP risks.

Figure 7: Actions Currently Pursued to Protect Product IP



Source: Aberdeen *Group*, November 2006

Given the relative strengths and weaknesses of each of these approaches, many companies are taking a blended approach. In fact, 82% are taking actions in at least two of the following three areas:

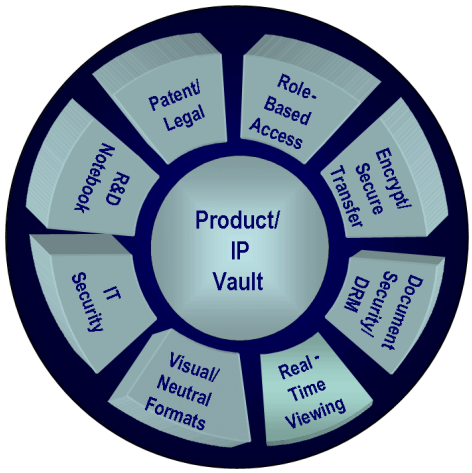
- Adopting "IP friendly" approaches to collaboration
- Better documenting IP discovery and enabling legal protection
- Improving product data protection, including enhancing IT security

Aberdeen's Framework for Protecting Product IP (Figure 8) was developed to help companies evaluate their own practices for protecting product IP. The framework encapsulates the three aspects of IP protection identified above. In particular, it includes.

- ***Product / IP vault*** – A secure repository for storing documents, designs, and related product data. The repository may be physical or logical in nature.
- ***Role-based access*** – Selective access to product information, typically through role-based access that determines what product, project, and specific elements are available to each authorized user as well as what actions he or she can take on this information.
- ***Secure transfer / encryption*** – Technology designed to protect designs and product data while in transit between partners. This may include automated capabilities for packing and distributing IP and tracking and audit capabilities.
- ***Document security / digital rights management (DRM)*** – For product data shared in documents and other files, security and access solutions that determine access and actions that can be taken on the information.

- ***Real-time viewing*** – Capabilities for viewing product data directly from the repository without distributing the information to collaboration partners.
- ***Visualization / neutral formats*** – Translation of design information into representations of the information. Representations may be in neutral, standard formats and typically allow for modifications to the level of detail and accuracy included.
- ***IT security*** – A broad category of solutions for securing and monitoring IT infrastructure including network security, electronic monitoring, and related capabilities.
- ***R&D notebook*** – Solutions that allow capturing and logging intellectual property research and discovery in order to support legal claims for IP invention.
- ***Patent / legal*** – IP asset management for documenting and managing patent applications, patents, and associated legal dockets.

Figure 8: Aberdeen's Framework for Protecting Product IP



Source: Aberdeen *Group*, November 2006

This framework can serve as a guide to companies when evaluating their strategies to protect IP. In addition, companies should understand what their peers are doing and which approaches are resulting in better protection.

"IP Friendly" Collaboration

The first approach explored is "IP friendly" collaboration. Working in cross-functional, globally dispersed teams is the reality for most companies today. To enable this, they must collaborate. But collaboration can be accomplished without sharing more information than is required for the partner to execute against its specific responsibilities.

The best way to protect product data is not to share it in the first place, but that is often not possible. However, as revealed in Aberdeen's *Global Product Design Benchmark Report*, many companies are sharing more information than required by their partners. Best in class companies are much more likely to take IP friendly approaches to collabora-

tion (Figure 9). For example, over one quarter of these leading companies share surfaces or volumes of items or components only. Often, partners need to understand the overall shape and function of a component, but not the internal complexity, which can be omitted. Product manufacturing information (PMI) can also be removed for partners who will not actually produce the items.

Another "IP friendly" approach is to limit the view to the "big picture" of the design. In particular, 21% of best in class companies (versus 13% of all others) are selectively providing segments of the overall product to specific partners, that is, "design partitioning." By controlling the overall product or systems-level design, companies can ensure that no one company understands the full interrelationships of the components.

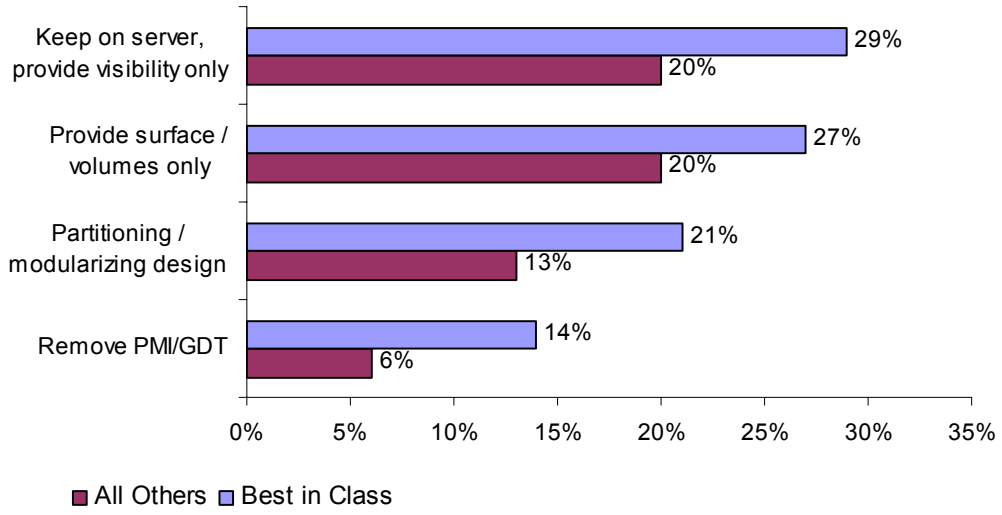
Case Study

"Our goal is that if someone really wants to reengineer a part, they will have to work from hardware instead of trying to leverage an electronic library of part geometry"

Complex Equipment

Beyond removing information, over one quarter of the companies indicated that they are not sharing design files with partners. Instead, they allow visibility to the designs only from the outside. In this way, the design file itself remains within the corporate firewall. Best in class companies are adopting these "IP friendly" approaches more frequently than their peers and competitors with lower levels of IP protection, leading to more secure product IP.

Figure 9: Leading Approaches to "IP Friendly" Collaboration

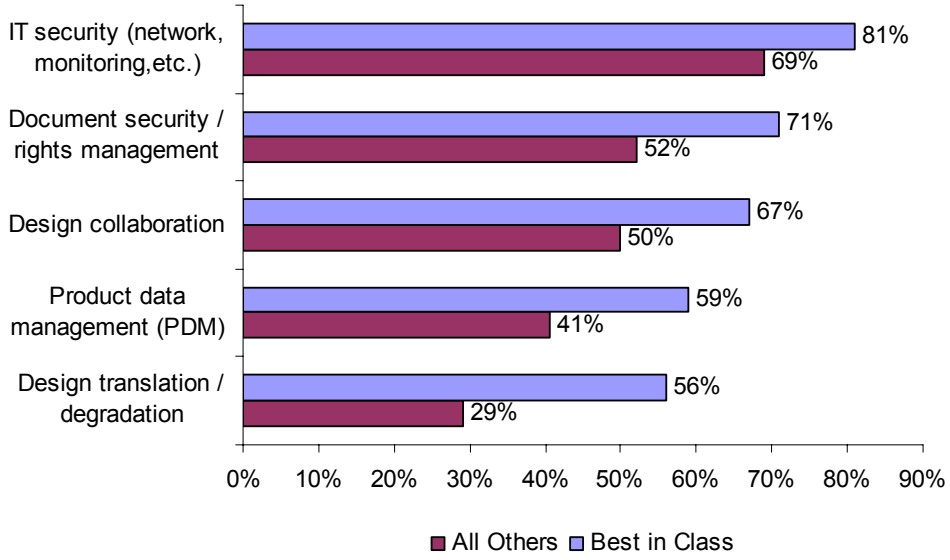


Source: Aberdeen *Group*, November 2006

In addition to adopting new business processes, leading companies are using product lifecycle management (PLM) and IT security technology to enable "IP friendly" collaboration (Figure 10). More than three quarters of the responding companies are utilizing IT security solutions such as network monitoring or other safeguards. Almost three quarters

are focusing on protecting design data that is stored in documents and files, utilizing digital rights management (DRM) solutions. Design collaboration technologies and product data management are also being used to help secure IP by enabling "IP friendly" approaches to collaboration. Some specialty solutions, such as design degradation, have been developed specifically to reduce the precision and content of product designs to prevent disclosure of IP. Enabling collaboration with the proper tools can help to ensure that collaboration is done in an effective – but also IP safe – way.

Figure 10: Technical Enablers for "IP Friendly" Collaboration



Source: Aberdeen *Group*, November 2006

Documenting and Protecting IP Discovery

Even when companies employ intelligent approaches to collaboration, products are still at risk of being copied or reverse engineered. To address this and discourage would-be IP thieves, legal protection is an important part of the overall IP protection strategy. The first step is documentation, such as recording discovery in an R&D notebook to document the finding. This document, with associated date stamps and signatures, can play a crucial role in protecting R&D value. Almost half of best in class companies, in fact, are utilizing electronic lab notebooks – twice the level of usage than in all other companies.

Beyond documenting their findings, best in class companies are also actively focusing on disclosing that information internally, so it can be reviewed for IP value. This review can result in a number of actions, including an application for patents or trademarks. In some cases, companies may choose to keep the information internal as a trade secret as opposed to filing for protection, allowing them to avoid public disclosure of the invention. According to benchmarks, best class companies are twice as likely as other companies to manage the review of invention disclosures.

Case Study

"We have had competitors import infringing devices from China. Our IP protection has allowed us to stop them or force significant modifications on their products"

Medical Devices

Documenting a discovery can provide protection in two ways. The first and most obvious way is to prevent others from using the information for their own advantage. The second is to defend the company should a competitor file a claim that its IP was infringed. In some cases, companies will patent a technology or simply publish a finding in order to enable their own legal defenses.

Should a company decide to protect a discovery, it must manage the process of applying for patents, trademarks, copyright, or other protection. Frequently, this protection must be filed in several countries and languages, resulting in multiple legal cases or related legal "dockets" that must be managed. Almost two thirds of best class companies surveyed are focused on managing applications for patents, trademarks, and other legal dockets.

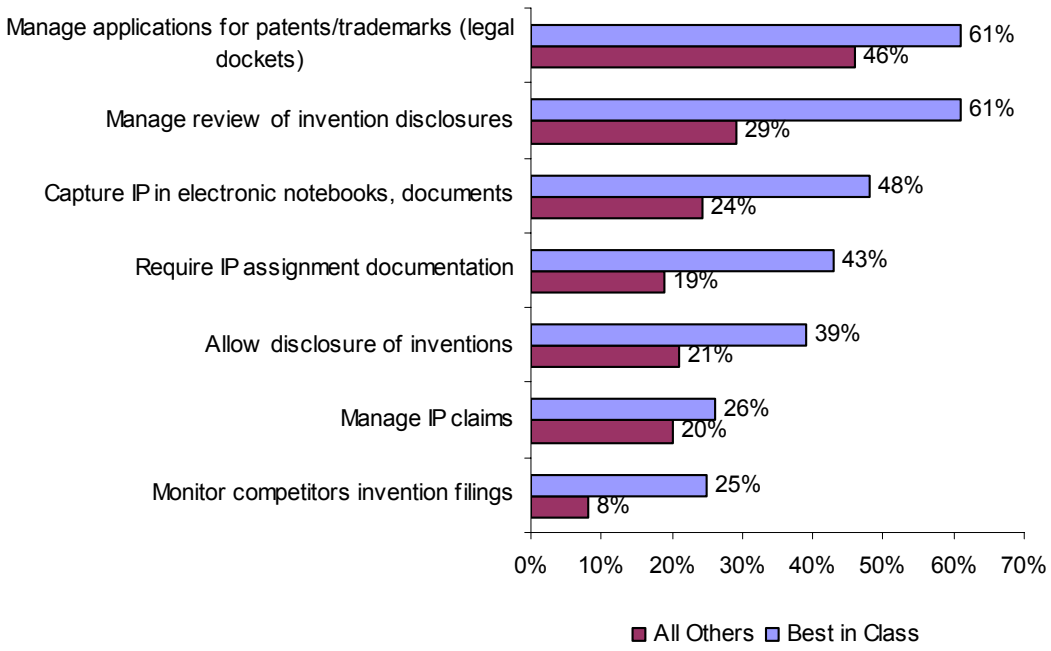
Case Study

"Our business has a high dependence upon technology and gains greater profits, we believe, from having a protected position gained from patents and proprietary knowledge."

Metals and Metal Products

Compared to all other companies, best in class companies are anywhere from 25% to over 200% more likely to be proactively managing the processes of documenting discovery, disclosing the findings, reviewing the disclosures to determine the approach for protection, and managing the applications for protection (or, alternatively, practicing defensive publishing) (Figure 11).

Figure 11: Leading Approaches to Protecting IP Discovery

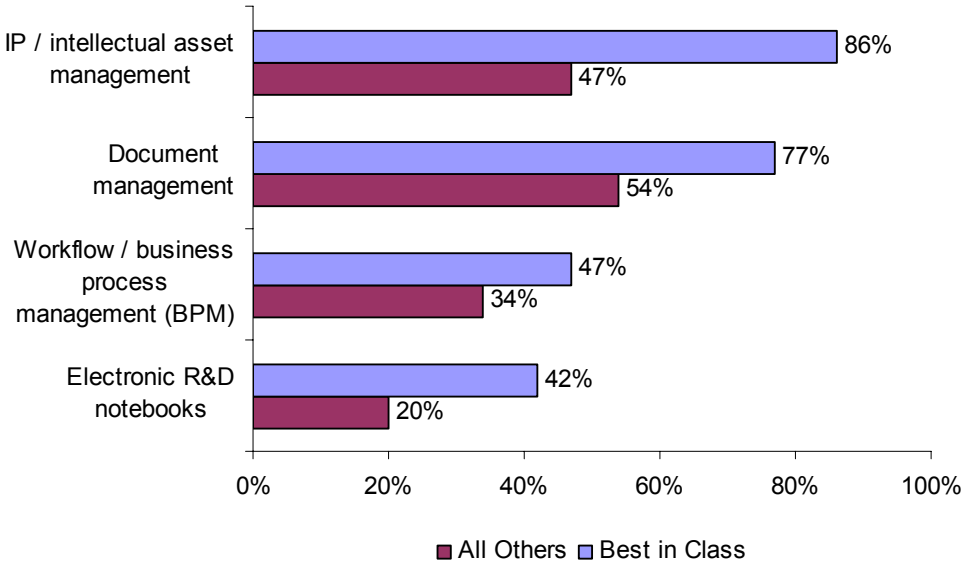


Source: Aberdeen *Group*, November 2006

Best in class companies are also more likely to be using technology to document discovery and legal protection, seeking to automate this process. Electronic approaches to documenting discovery offer the ability to maintain legal protection, but also promote internal reuse of discovery. Best in class companies clearly recognize this, as they are twice as likely to utilize electronics R&D notebook technology. Similarly, encouraging easy disclosure of inventions leads to better IP use and protection. Finally, companies must manage the complex processes and multiple dockets associated with legal protection. Best in class companies are 83% more likely to use intellectual asset management solutions than other companies.

In fact, best in class are adopting technology to help them better identify, disclose, and protect IP discoveries and the associated product IP (Figure 12). These technologies include specialized tools, as well as more general solutions such as document management and workflow systems that can be used to enable legal protection.

Figure 12: Technical Enablers for Protecting IP Discovery



Source: Aberdeen *Group*, November 2006

Safeguarding Product Data

The third best practice identified is protecting product data. Because of easy data access and transportability, the need to ensure that only the intended audience is accessing the information – and with the right privileges – is critical. The first line of defense is typically general IT security (pursued by over three quarters of best in class companies), including network monitoring and threat detection.

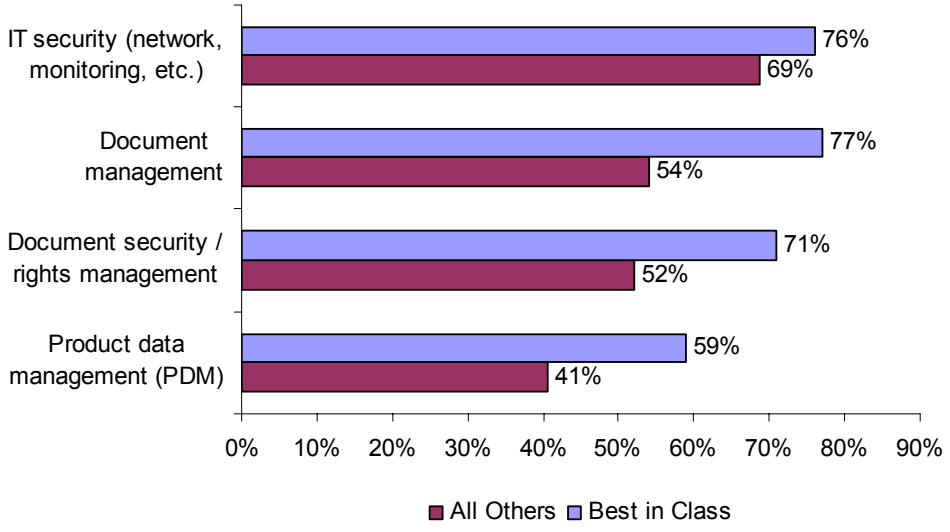
Data security must be controlled in a collaborative environment, balancing access with protection. Product data management (PDM) and document management systems (used

by 59% and 77% of the best in class, respectively) can provide role-based security features that dictate who has rights to what information. PLM providers offer this access with respect to role, product, project, company, and other attributes. Some solutions provide the ability to restrict specific data elements within a product. However, this approach must be enabled with a security model that meets the realities of today's design environment. If the solution is not well defined, the level of effort required to protect IP will inhibit its use and protection will be bypassed.

One newer area of concern is the ease of communicating design data in documents and files. *The Global Product Design Benchmark Report* indicated that the most common technologies used to enable global design are e-mail and documents. Because of the ease of copying data to portable drives, e-mailing the information, or even burning compacts disks (CDs), the need to protect data found in documents and files is increasing. Digital rights management (DRM), which is being pursued by 71% of best in class companies as compared to 52% of all others, is a critical component of any IP strategy. Given the need to communicate with broad audiences and short product development windows, document-based collaboration is a natural process. There are now emerging technologies that can be deployed to protect the technical contents of documents and files that have been passed to others for collaborative purposes – or have been intercepted or received by unintended parties such as competitors.

Best in class companies, those that report higher levels of IP protection, are focusing on keeping product data secure – both inside and outside of the firewall (Figure 13).

Figure 13: Technical Enablers for Protecting Product Data



Source: Aberdeen *Group*, November 2006

Chapter Three:
Implications & Analysis

Key Takeaways

- Best in class companies make a key executive responsible for protecting IP.
- Best in class businesses adopt more formal business processes to protect product IP and incorporate them in their new product development (NPD) processes.
- Best in class companies measure performance in IP protection more frequently, although IP protection is not routinely measured by most companies.
- Best in class companies coordinate and integrate their technology strategy for product IP protection and leverage a variety of software technologies to achieve their superior performance.

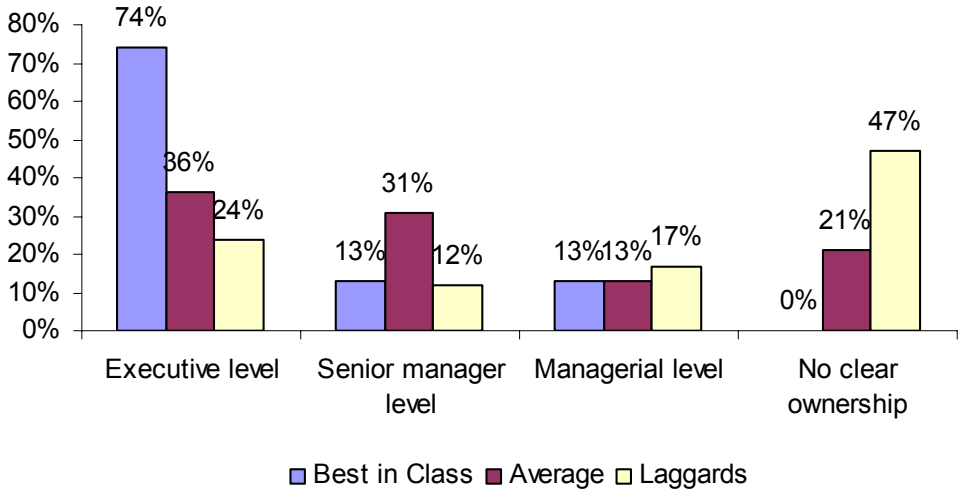
Best in class companies are taking proactive steps to enable themselves for IP protection. As described in Chapter 2, leading companies are aggressively seeking IP protection by adopting best practice processes and technology. These must be coupled with the appropriate business capabilities, however, in order to provide value. Aberdeen research indicates that companies with the best reported IP protection, the best in class, have taken different approaches in each of these facets of their business.

Best Practice: Executive Ownership of IP Protection

Protecting product information crosses departmental boundaries and impacts both product development participants and information technology (IT). In addition, protecting IP must be balanced with very strong pressures within product-driven companies, namely for product innovation and shorter time to market. Given this potential for conflicts, it is easy to see why leading companies place responsibility for IP at a very senior level in their organizations.

In fact, leading companies are twice as likely as average companies – and a full three times as likely as laggards – to have IP responsibility at an executive level (Figure 14). On the contrary, almost half of the laggards not only lack executive leadership; they report that they have no clear ownership of protecting product IP at all.

Figure 14: Organizational Strategies for Protecting Product IP



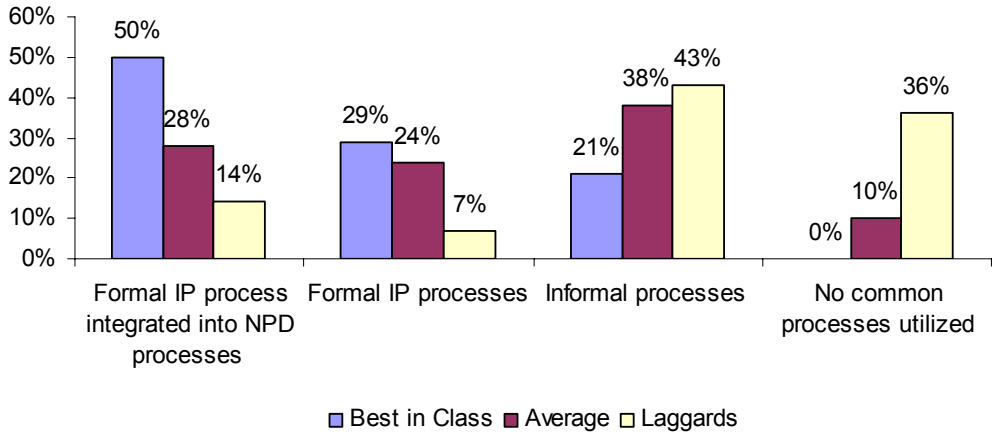
Source: Aberdeen *Group*, November 2006

Best Practice: Formalizing and Integrating IP Protection Practices

Protecting IP requires organizational discipline, which has led best in class companies to implement formalized processes to protect product IP. Without these processes, individuals and teams would be responsible for developing their own practices – leading to suboptimal and conflicting processes as well as inefficiency. Over three quarters of best in class companies indicate that they have formal IP processes (Figure 15). In stark contrast, three quarters of laggard performers report informal processes or no common processes.

Beyond formalizing processes, a full 50% of best-in-class performers indicate that they have integrated their IP processes into their overall new product development (NPD) processes. This integration helps to ensure that IP protection is an integral part of the daily routine, as opposed to an afterthought or some additional work that needs to be accomplished at day's end. Average companies, on the other hand, are only 28% likely to have integrated IP and NPD processes, with laggards indicating only half of that level.

Figure 15: Business Process Strategies for Protecting Product IP

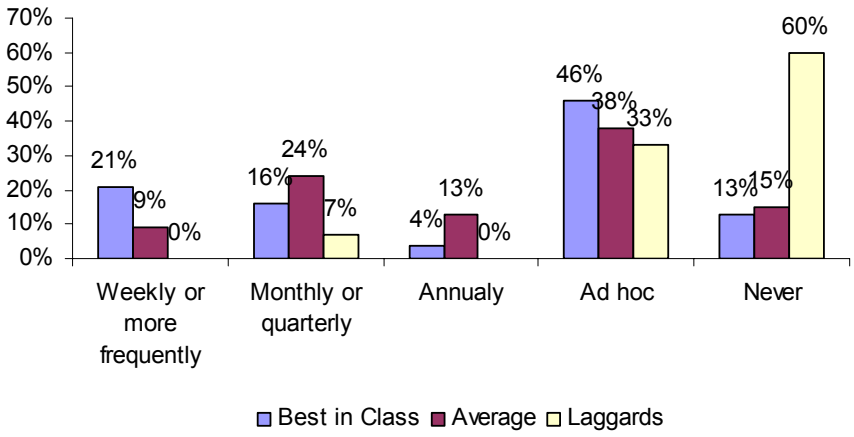


Source: Aberdeen *Group*, November 2006

Best Practice: Measuring IP Protection Performance

Aberdeen research findings also reveal that leading companies are twice as likely to measure IP performance on at least a weekly frequency (Figure 16). While this finding indicates that performance measurement is more common in best in class companies, it should also be noted that even for these leaders the majority report that they are measuring IP performance on an "ad hoc" basis if at all. Consequently, there is significant room for improvement in many companies' approaches to determining the successfulness of their IP protection.

Figure 16: Performance Measurement Frequency for Protecting Product IP



Source: Aberdeen *Group*, November 2006

Best Practice: Coordinating and Integrating Technology Strategy

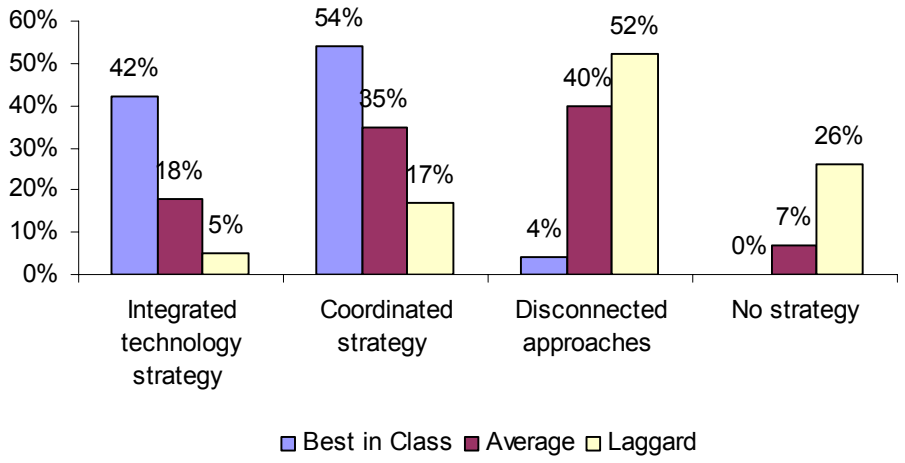
Best in class are coordinating and integrating their technology strategy for IP protection in addition to adopting process-oriented approaches. Business enablers such as organizational ownership, implementing leading business processes, and measuring performance all play a key role in enabling best in class IP protection, but technology is frequently the vehicle for executing these safeguards. Product IP is now better documented digitally, making it an important electronic asset.

In fact, the previous chapter discussed the importance of automated solutions in each of the three main areas of protecting product IP. A wide variety of technical enablers were identified as being favored by best-in-class companies, including:

- IT security
- Digital / document rights management (DRM)
- Product data management (PDM)
- Design collaboration
- Design translation / degradation
- IP / Intellectual asset management solutions
- Document management
- Workflow / business process management (BPM)
- Electronic R&D notebooks

Aberdeen research shows that beyond implementing these individual solutions, best in class companies are much more likely to have coordinated – or even integrated – their various technology strategies to protect product IP (Figure 17). A coordinated approach considers multiple aspects of IP security independently. While all of the solutions may not be technically integrated, different security approaches are developed to complement each other.

Figure 17: Technology Strategy for Protecting Product IP



Source: Aberdeen *Group*, November 2006

In summary, benchmarks show that best in class performers have adopted coordinated – if not integrated – technology strategies to protect product IP. In fact, it is by adopting organizational structures, processes, performance measurement, and technologies that promote IP protection – in combination – that these companies have achieved their best in class level of success in IP protection.

Chapter Four: Recommendations for Action

Key Takeaways

- Adopt "IP friendly" approaches to collaboration to enable global design and manufacturing with partners while maintaining control of and protecting product IP.
- Document IP discovery and develop strategies for legal protection that include proactive steps for legal protection from both IP infringement and infringement claims from others.
- Ensure safeguarding of product data including implementing enhanced IT security to secure product data within the firewall and digital rights management (DRM) to protect product IP "in the wild" when designs are shared outside of the corporate firewall.
- Place a senior executive in charge of IP protection.
- Formalize IP protection processes, and integrate them with overall new product development (NPD) processes.
- Develop an integrated technology strategy for IP protection, considering the combined aspects of "IP friendly" collaboration, documenting discovery, legal protection, and safeguarding product data both inside and outside the firewall.

Protecting IP is a "top five" strategy for leading manufacturers. Best in class companies have developed legal, business process, and technical strategies that help them achieve higher levels of performance in protecting their IP assets. These strategies and actions are paying off (as reported in Figure 1, Executive Summary) as best in class companies are over five times more likely to report significant gains in IP protection than the poorest performers.

To obtain these benefits, companies must first assess their current level of performance and then determine the path to maturing to the next level. Whether a company is trying to gradually move its IP protection from "Laggard" to "Industry Average," or "Industry Average" to "Best in Class," the following actions will help spur the necessary performance improvements:

Steps to Success for All Companies

1. *Adopt "IP friendly" approaches to collaboration.*

   All companies should strive to strike a strategic balance between enabling effective product innovation, product development, engineering, and manufacturing and protecting IP. Approaches to product lifecycle collaboration should be tailored in order to share the right amount of information with the right partners – and no more. Approaches that should be considered include "dumbing down" designs shared with partners by providing surface areas only, stripping out manufacturing information, decreasing the precision of the information, or even purposefully removing or altering features. In addition, designs can be shared by streaming, as opposed to sharing, a file, or files can be encrypted and protected.

Finally, design partitioning can be used to ensure that only a select number of individuals can view the entire product in its entirety.

2. *Document and protect R&D discoveries.*

   All companies should ensure R&D discoveries are captured, evaluated from a business perspective, and safeguarded by executing the appropriate protection (i.e., patents, trademarks, trade secrets, defensive publishing). Product IP should be managed as an asset, and all associated applications for patents and other legal dockets should be controlled and managed. Legal protections such as IP assignment documentation and non-disclosure agreements should be put in place to further legal protection.

3. *Enhance product data protection inside and outside of the firewall.*

   All companies must ensure that data is effectively safeguarded. Effective product data management and vaulting techniques, including fine-grained security based on roles, products, and projects, should be applied to limit product data access to authorized parties. Focusing on overall IT security is also a must for protecting data. The IP protection strategy should also include rights management capabilities to protect product IP "in the wild" when designs are shared with others outside of the corporate firewall.

Laggard Steps to Success

1. *Establish clear ownership for IP protection.*

   Assign direct ownership of IP protection to an individual who can take charge of processes and technology related to protecting product IP. Centralizing control of IP processes and strategy allows for a more holistic, integrated approach that spans departmental and corporate boundaries.

2. *Develop and formalize common processes for IP protections*

   Develop formal, standardized processes for the protection of product IP so that decisions about appropriate approaches to sharing IP are not left up to individuals who are faced with deadlines and may be willing to take a shortcut if not instructed otherwise. Common processes also provide a foundation for reviewing and improving processes over time and sharing best practices and technology across organizations or departments.

3. *Define a formal technology strategy for protecting product IP, and coordinate the strategy to ensure multiple aspects of IP security are developed to complement each other.*

   Recognize the importance of technology in protecting IP, and define a technology strategy if one does not already exist. Ensure that the new or existing strategy coordinates disparate activities related to protecting IP. View IP protection as a combined solution that is more powerful as a whole than as individual elements. The combined strategy should consider best in class technologies such as elements of IT security, PLM, collaboration tools, design translation, digital rights management (DRM), workflow, electronic R&D notebooks, IP asset management, and potentially other solutions.

Industry Norm Steps to Success

1. *Establish executive ownership for IP protections*

   Assign direct ownership of IP protection to an executive who can take charge of processes and technology related to protecting product IP. Centralizing control of IP process and strategy allows for a more holistic, integrated approach that spans departmental and corporate boundaries. Placing an executive in charge allows IP protection to be elevated to the appropriate level, so it can be balanced with strong forces such as time to market and product innovation pressures.

2. *Formalize common processes for IP protection and integrate these processes with the overall new product develop (NPD) process.*

   Develop formal, standardized processes for the protection of product IP so that decisions about appropriate approaches to sharing IP are not left up to individuals who are faced with deadlines and may be willing to take a shortcut if not instructed otherwise. Common processes also provide a foundation for reviewing and improving processes over time and for sharing best practices and technology across organizations or departments. To ensure adoption of these processes, integrate them with existing NPD processes to make protecting IP a normal part of the business workflow.

3. *Define a formal technology strategy for protecting product IP, and coordinate the strategy to ensure multiple aspects of IP security are developed to complement each other.*

   Recognize the importance of technology in protecting IP, and coordinate disparate activities. View IP protection as a combined solution that is more powerful as a whole than as individual elements. The combined strategy should consider best in class technologies such as elements of IT security, PLM, collaboration tools, design translation, digital rights management (DRM), workflow, electronic R&D notebooks, IP asset management, and potentially other solutions.

Best in Class Next Steps

1. *Integrate product IP protection processes with the overall new product develop (NPD) process.*

   To ensure adoption of IP protection processes and make them a normal part of the business workflow, integrate them with existing NPD processes. Leverage existing business process capabilities such as workflow and employee training to ensure IP protect is a part of the standard operating procedures of the company.

   .

Featured Underwriters

This research report was made possible, in part, with the financial support of our underwriters. These individuals and organizations share Aberdeen's vision of bringing fact based research to corporations worldwide at little or no cost. Underwriters have no editorial or research rights and the facts and analysis of this report remain an exclusive production and product of Aberdeen Group.

Adobe

Adobe revolutionizes how the world engages with ideas and information. For more than two decades, the company's award-winning software and technologies have set new standards for producing and delivering content that engages people virtually anywhere at anytime. From rich images in print, video, and film to dynamic digital content across multiple media, the impact of Adobe solutions is evident across industries and felt by anyone who creates, views, and interacts with information. With a reputation for excellence and a portfolio of many of the most respected software brands, Adobe is one of the world's largest and most diversified software companies.

For additional information on Adobe Systems Incorporated:
345 Park Avenue, San Jose, CA 95110-2704
888-649-2990; 408-536-6000;
www.adobe.com/manufacturing

Agile Software Corporation (NASDAQ: AGIL) helps companies drive profits, accelerate innovation, reduce costs, and ensure regulatory compliance throughout the product lifecycle. With a broad suite of enterprise-class PLM solutions and time-to-value focused implementations, Agile helps companies get the most from their products. Small and medium enterprises including Colubris Networks, McAfee, Ondine Biopharma, OnStor, Sonic Innovations, Visx, as well as large and global enterprises such as Alcatel, Boeing, Dell Inc., Flextronics International, Hitachi, Leapfrog, Lockheed Martin, Magna Steyr, Siemens, QUALCOMM and ZF are among the nearly 10,000 customers that license Agile solutions. Agile OnDemand is a Software as a Service (SaaS) version of the Agile Advantage solution. Agile also offers an Agile OnDemand PLM Small Business Startup Pack, at no charge, for qualified customers in the small enterprise market. Agile OnDemand is the lowest total cost of ownership PLM solution.

For additional information on Agile Software Corporation::
6373 San Ignacio Avenue, San Jose, CA 95119-1200
408-284-4000
www.agile.com

Linx/AS™
Envision PLM

Linx/AS LLC is a leading Product Lifecycle Management (PLM) consulting firm that provides: strategic planning through a proprietary PLM Vision™ Methodology; expert SAP integration services; SAP-certified product innovations; and hands-on training. Linx/AS has successfully helped small- to mid-sized businesses up to Global 2000 companies maximize their ROI in SAP technology and lower the TCO for IT organizations. Linx/AS experience spans verticals with a focus on process industry. As a thought-leader in innovation management, Linx/AS offers Intellectual Property Manager--a Powered by SAP NetWeaver™ solution that helps companies strategically inventory, valuate, and protect their IP portfolio on an enterprise level.

For additional information on Linx/AS LLC::
610 Freedom Business Center, Suite 100, King of Prussia, PA 19406
610-992-9333; info@linxas.com
www.linxas.com

Pinion Software is the leading provider of information security solutions for the emerging Technical Rights Management (TRM) marketplace. The company's software products protect high-value intellectual property during design collaboration, outsourced manufacturing, and other technical business processes where digital data must be shared. Users of CAD, other technical, and business applications can create and share files in their native application format while retaining continuous control over how the information is used by recipients. Pinion Software protects information both inside and outside the corporate firewall - whether shared by email, CD/DVD, Product Lifecycle Management, portal, or other technical data management system.

For additional information on Pinion Software:
12885 Research Boulevard, Suite 204, Austin, TX 78750
512-583-5000; sales@pinionsoftware.com
www.pinionsoftware.com

Based in Los Altos, CA, Radiance Technologies is a breakthrough company delivering Managed Asset Delivery solutions that enable users and organizations to send, receive and collaborate on large content between remote locations around the world with unparalleled ease. Radiance's Courier™ and TrueDelivery™ systems provide comprehensive tracking and monitoring, guaranteed reliability all with US DoD certified security. Radiance was founded in 2000, and its investors include Levensohn Venture Partners, Vanguard Ventures and Sutter Hill Ventures.

For additional information on Radiance Technologies:
5050 El Camino Real, Suite221, Los Altos, CA 94022
650-625-9510; sales@radiance.com
www.radiance.com

Appendix A:
Research Methodology

Between October and November 2006, Aberdeen Group examined the product intellectual property protection procedures, experiences, and intentions of approximately 150 enterprises in a wide range of manufacturing industries.

Responding participants completed an online survey that included questions designed to determine the following:

- The current challenges to protecting product IP in global markets.
- The effectiveness of existing product IP procedures and infrastructures.
- The use of automation to aid their product IP protection initiatives.
- The results and benefits of successful technology, organizational, and process approaches aimed at improving product IP protection.

The study aimed to identify emerging best practices for protecting product IP and provide a framework by which readers could assess their own IP protection capabilities.

Responding enterprises included the following:

- ***Job title/function:*** The research sample included respondents with the following job titles: manager (38%); senior management such as CEO, CFO, COO (20%); staff (14%); Director (13%), Vice President (7%), internal consultant (5%), and CIO/IT Leader (3%). Respondents represented Engineering (43%), Information Technology (13%), Business Process Management (10%), Marketing (9%), Procurement (7%), Logistics/Supply Chain (5%), Manufacturing (4%), Quality (3%), Legal (2%), Finance (2%), and others (2%).
- ***Industry:*** The research sample included respondents from diverse discrete, process, and consumer manufacturers. These included 17% from industrial equipment manufacturers, 11% from high-tech/software; 9% from aerospace and defense; 8% from engineering firms, 7% from both computer equipment peripherals and medical devices; 6% from automotive, 5% from telecommunications equipment, 6% from consumer goods, 4% from food and beverage,; and the remainder from various other industries.
- ***Geography:*** A majority of study respondents (74%) were from North America. Remaining respondents were from Europe (14%); Asia-Pacific (9%); Central and South America and the Caribbean (2%); and the Middle East and Africa (1%).
- ***Company size:*** Overall, 21% of respondents were from large enterprises (annual revenues above US$1 billion); 39% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 42% of respondents were from small businesses (annual revenues of $50 million or less).

Solution providers recognized as sponsors of this report were solicited after the fact and had no substantive influence on the direction of *The Product Intellectual Protection*

Benchmark Report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

Table 2: PACE Framework

PACE Key
Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows: *Pressures* — external forces that impact an organization's market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive) *Actions* — the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product/service strategy, target markets, financial strategy, go-to-market, and sales strategy) *Capabilities* — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products/services, ecosystem partners, financing) *Enablers* — the key functionality of technology solutions required to support the organization's enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)

Source: Aberdeen Group, November 2006

Table 3: Relationship between PACE and Competitive Framework

PACE and Competitive Framework How They Interact
Aberdeen research indicates that companies that identify the most impactful pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute.

Source: Aberdeen Group, November 2006

Table 4: Competitive Framework

Competitive Framework Key
The Aberdeen Competitive Framework defines enterprises as falling into one of the three following levels of product IP protection practices and performance: *Laggards (30%)* — product IP protection practices that are significantly behind the average of the industry, and result in below average performance *Industry norm (50%)* — product IP protection practices that represent the average or norm, and result in average industry performance. *Best in class (20%)* — product IP protection practices that are the best currently being employed and significantly superior to the industry norm, and result in the top industry performance.

Source: Aberdeen Group, November 2006

Appendix B:
Related Aberdeen Research & Tools

Related Aberdeen research that forms a companion or reference to this report includes:

- *The Product Innovation Benchmark Report* (September 2005)
- *The Global Product Design Benchmark Report* (December 2005)
- *The Product Collaboration Benchmark Report* (June 2006)

Information on these and any other Aberdeen publications can be found at www.Aberdeen.com.

Aberdeen Group, Inc.
260 Franklin Street
Boston, Massachusetts
02110-3112
USA

Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

November 2006

Founded in 1988, Aberdeen Group is the technology-driven research destination of choice for the global business executive. Aberdeen Group has over 100,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services.

THIS DOCUMENT IS FOR ELECTRONIC DELIVERY ONLY

The following acts are strictly prohibited:

- **Reproduction for Sale**
- **Transmittal via the Internet**

Terms and Conditions

Upon receipt of this electronic report, it is understood that the user will and must fully comply with the terms of purchase as stipulated in the Purchase Agreement signed by the user or by an authorized representative of the user's organization. Aberdeen has granted this client permission to post this report on its Web site.

All information contained in this report is current as of publication date. Information contained in this publication has been obtained from sources Aberdeen believes to be reliable, but is not warranted by the publisher. Opinions reflect judgment at the time of publication and are subject to change without notice.

Usage Tips

Report viewing in this PDF format offers several benefits:

- **Table of Contents:** A dynamic Table of Contents (TOC) helps you navigate through the report. Simply select "Show Bookmarks" from the "Windows" menu, or click on the bookmark icon (fourth icon from the left on the standard toolbar) to access this feature. The TOC is both expandable and collapsible; simply click on the plus sign to the left of the chapter titles listed in the TOC. This feature enables you to change your view of the TOC, depending on whether you would rather see an overview of the report or focus on any given chapter in greater depth.
- **Scroll Bar:** Another online navigation feature can be accessed from the scroll bar to the right of your document window. By dragging the scroll bar, you can easily navigate through the entire document page by page. If you continue to press the mouse button while dragging the scroll bar, Acrobat Reader will list each page number as you scroll. This feature is helpful if you are searching for a specific page reference.
- **Text-Based Searching:** The PDF format also offers online text-based searching capabilities. This can be a great asset if you are searching for references to a specific type of technology or any other elements within the report.
- **Reader Guide:** To further explore the benefits of the PDF file format, please consult the Reader Guide available from the Help menu.