WHITE PAPER

NEXTLABS

Intellectual Property Protection

BEST PRACTICES FOR PROTECTING INTELLECTUAL PROPERTY

INTRODUCTION

No single company has the capability to design and manufacturer all of the complex technical components found within today's automobiles, airplanes, chemicals, computer systems, or electronic devices. As products become more complex companies find themselves in increasingly distributed and collaborative supply chains. Collaborative supply chains offer great benefits, including efficiency, flexibility, lower costs, and increased levels of innovation. At the same time, however, companies take on greater risk by relinquishing control over processes, materials and intellectual property (IP). Much has been written about the supply chain risks associated with materials, but the risk associated with IP is just as great. Your digital IP is being copied and shared dozens or hundreds of times, and any mishandling could have severe impact to your business. Fortunately, every challenge presents an opportunity. Companies are more dependent on one another and those who do a better job of managing IP risk by protecting company, customer, and supplier IP are able to garner greater loyalty as a trusted business partner.

This paper describes some of the key challenges to protecting IP within the collaborative supply chain, outlines ten real-world best practices for managing those risks, and describes the NextLabs' solution for implementing those best practices.

IP PROTECTION CHALLENGES

NextLabs has worked with large manufacturing organizations in High Tech, Capital Equipment, Aerospace and Defense, and Chemical industries on protecting IP within collaborative supply chains. We have seen four common business contexts where companies struggle with IP protection.

Outsourced Manufacturing

Outsourced manufacturing allows companies to lower costs and utilize cutting-edge technologies. When OEMs outsource manufacturing of components to one or more contract manufacturers, they need to share large amounts of product data, process data, specifications, and designs. OEMs need to ensure that the appropriate level of IP is being shared with each manufacturer. Likewise, contract manufacturers need to ensure that their customer's IP is properly protected within their organizations. To ensure proper data handling, many OEMs audit contract manufacturing organizations.

Global Product Development

Global product development allows companies to lower costs and tap into global talent. However, when a company establishes design, development, or manufacturing in global locations they need to address the associated compliance and information risk. Regulatory requirements make managing and sharing trade-restricted data between countries much more complex, and many countries do not provide the same level of governmental or legal protections for IP.

Mobile Workforce or Mobile Data

Mobility allows companies to leverage talented resources anywhere in the world and allows employees greater flexibility and productivity. However, this mobile workflow also takes company IP on the road, often on unprotected laptops, mobile devices, or removable storage that can easily be lost or stolen.

Collaborative Technologies

Collaborative technologies such as email, instant messaging, Microsoft SharePoint, extranet portals, and software-as-a-service (SaaS) applications make it easier to share information and communicate in¬novations. Many of these products are based on ad-hoc administrative models and discretionary access controls. Moreover, they often lack mandatory controls over what information can be share with whom, making it difficult to distinguish between authorized external collaboration and external data loss.

One common theme found in these four scenarios is the ease with which IP can be transformed, duplicated and shared. Protecting IP requires us to consider the data itself as it moves between applications, systems, users, and organizations.

IP PROTECTION BEST PRACTICES

In the collaborative supply chain, companies cannot simply lock their data in a safe. Instead, organizations need to take a risk management approach to IP protection: identify risks, tackle the largest ones first, design controls (policies and procedures) to address those risks, implement and audit the effectiveness of these controls, and repeat as necessary.

Universally we see the same IP risks showing up at the top of the list: lack of data identification; product development in trade restricted countries where legal protections are inadequate; data leakage beyond project teams, due to mishandling; insecure or unmonitored data transfer or distribution between supply chain partners; and data lost on unprotected laptops, removable drives, or mobile devices.

In this section we present ten of the best practices developed by working closely with customers to protect IP.

Take a data-centric approach.

Traditional security technologies focus on a specific application, infrastructure, or the network perimeter -- for example, access controls within a PLM application, or network intrusion prevention products. In the collaborative supply chain, however, data needs to moves across systems and corporate network boundaries. In order to protect IP one must focus on the data, which can easily be downloaded, transformed, copied, and shared. So protection must span applications, servers, desktops, and communication channels.

Label data with business attributes.

While it may sound surprising, it is very common for a company to say, "we have no idea what data we have and how it is classified." Many companies have a four- to six-level data classification scheme derived from government classification systems and based on data sensitivity. For example one common scheme is: Public, Company Confidential, Third-Party Confidential, Restricted, and Highly Restricted.

Unfortunately, this type of classification is almost impossible for end users to apply, which serves to compound the classification problem. The guidelines for what data is Confidential and what data is Restricted are often non-prescriptive and a single document's classification can change several times over its lifecycle. For example, a product data sheet is probably considered Restricted before a product launch and then considered Public once it is placed on the website.

It is more reasonable to ask end users to label data with business attributes. What type of data or document is it? What product or project is it for? What organization does it belong to? These attributes change infrequently and are easy for end users to apply. The data sensitivity level and associated policy can be derived from these business attributes.

Establish clear policy for IP handling.

One of the top reasons why employees put IP at risk is because they don't understand the rules. Writ¬ten policy is generally far from black and white. Clear, simple, and easy-to-remember policies should be established to ensure that the appropriate protection is applied to IP as it is created, stored, and shared. Policy should be set to guide users in making decisions regarding:

Labeling - How and when to label or classify data

Storage/Management - Where to store certain classes of data, including the appropriate system-of-record, desktops, laptops, mobile devices, and removable storage

Distribution - Appropriate use of collaboration technologies (email, instant messaging, web meetings, Microsoft SharePoint, and SaaS applications) for the distribution of IP between internal groups and external partners or customers

Access Control and Document Rights - Clear procedures and rules for authorizing and deauthorizing users to access IP is critical. Access should be based on what someone needs to do their job and their attributes (e.g. clearance level, training, or citizenship). Just leaving it up to "manager approval" will lead to too much access.

Enforce policy.

With clear policy defined it is now possible to actually enforce it. There are a number of tools that can be used to enforce controls. These range from simple access controls to more sophisticated data protection or data loss prevention products. When looking for a control implementation solution, you should be sure that your choice can meet your current policy requirements and is also flexible enough to meet future requirements, which may be driven by new business partnerships or the introduction of new collaboration applications.

Provide just-in-time education on proper data handling.

Once you have policy established, users need to be educated so that they can comply. Many companies provide training to users when they first join a company and then only periodically when policies are amended or modified. This level of education is necessary, but not sufficient. End users need to understand not only what the policy says, but also how to apply it and use it to guide their decisions and actions when actually doing their work. Educating users on the application of policy needs to happen just-in-time – when the user is about to click the send button on the email message.

Automate procedures - make it easy for users to comply with policy.

Users are often faced with situations where following policy or manual procedures is simply too onerous. These procedures may stand between the user and an important business transaction or simply impede their productivity. In these cases, users will almost always choose "getting it done" over "doing it right". To avoid this, IP protection procedures should be automated where possible, so that end users do not need to make this trade-off.

Monitor activity, and let users know you are doing it.

Having visibility into the access, use, and sharing of your sensitive IP is critical. Many companies employ an incident response philosophy where IP breaches are investigated and users are held accountable. Unfortunately, this approach is often too little too late. The IP is already compromised and users are investigated as suspects, not trusted employees, partners, or customers. Remember that the goal is to reduce risk, not spy on employees. A more cost-effective approach is to monitor critical user activity and analyze the information so you can detect abnormal behavior and predict possible IP loss before it occurs. We have found that if you let your employees know that you are monitoring, end users will instinctively be more careful. Keep in mind that activity monitoring may be subject to employee privacy laws, so you may need to tailor your strategy based on the regulations in different countries or regions.

Manage lists of external parties and the project level.

Being good at external collaboration is the key to becoming a trusted partner within the collaborative supply chain. However, allowing indiscriminate sharing of external data can open you up to significant risk of IP loss. One issue we see is that many companies do not have a system to track which companies and individuals at those companies are authorized for collaboration projects. Project Managers will generally have some tacit knowledge of external parties involved in their project, but lack a system where this information can be easily created and managed. Once you have this system, it becomes possible to limit sharing of project data with authorized parties, allowing you to increase the total level of collaboration.

Continuously audit the effectiveness of policy.

Once controls (policy and procedures) have been implemented, they need to be periodically audited to ensure that they are in use and effective in meeting the stated control objective. Typically this is done by an internal or external audit team, who is provided the control definitions and access to users and systems to observe the control implementation. When handled as a manual process, auditing can be quite labor intensive. We have found that it is better to continuously audit, by automating the capture of required audit data, rather than perform audits on a quarterly or semi-annual basis.

Start small but think long term.

For most companies, it is not practical to tackle the end-to-end IP protection problem. The problem is too vast, and trying to find a silver bullet can lead to organizational paralysis. Today's companies often comprise several business units that were perhaps acquired or merged over time. A big-bang solution to IP protection will likely not succeed, since different teams use different applications and processes.

To move forward it is better to identity one area, such as a division or project, which has high value IP at risk and start there. At the same time, however, when you develop the solution platform you need to think long term. The solution you deploy needs to be flexible and extensible enough to meet the requirements of other divisions and projects. If it is not, you may end up with tens or hundreds of independent solutions to manage.

SOLUTION FOR IP PROTECTION IN THE COLLABORATIVE SUPPLY CHAIN

NextLabs provides a number of applications for both OEMs and contract manufacturers that help companies manage IP risk. Each application provides prebuilt controls (policies and procedures) and audit reports that can be automatically enforced by our products, NextLabs Entitlement Management and NextLabs Data Protection. Both products run on the same Policy Server Platform, based on the XACML policy standard and integrated workflow. For companies looking for ways to protect data within the collaborative supply chain, the NextLabs' products can help with applications for:

IP Classification and Tagging

Automatically apply labels or tags to documents as they are created, stored or shared, to facilitate discovery and control. Tags can be automatically applied based on identity, context, and content, or end users can be prompted to apply required tags as they save documents. For example:

Whenever a CAD drawing is copied to a project file server, automatically tag the drawing with a project designation.

Whenever a design document is created that contains a specific part number, automatically tag the document with the associated product designation.

Whenever a member of the Finance organization saves a spreadsheet that contains financial data prompt him or her to indicate whether the document contains corporate financial data.

IP Activity Monitoring, Audit, and Reporting

Automatically monitor user access, usage, storage, and sharing of IP data. Measure policy violations to audit their effectiveness. Prebuilt dashboards, charts, and reports highlight important trends and key compliance indicators and allow analyst to slice and dice activity data for investigations.

Project-Based Access and Document Control

Control access to IP across multiple heterogeneous applications or systems based on project assignments for employees, supply chain partners and customers. Manage a single set of policies that govern access to IP sitting on FTP sites, file servers, document management systems, and Microsoft SharePoint sites.

Access rights change automatically as individuals are assigned or removed from projects, without the need to create or manage separate groups in Active Directory or modify identity management roles.

All IP access and use can be monitored and logged to a central activity journal where it can be easily reported on for internal, external, or customer IP audits or investigations.

Project Information Barriers

Document controls allow you to also apply policy to limit how IP documents can be used, stored, duplicated and shared to prevent leakage of data to unauthorized employees, contractors, customers, or partners. Policy-based information barriers can be defined around project data to limit storage on various systems or within particular application folders, such as a SharePoint site, file share, or FTP site, and to control sharing of data with particular users, both internal and external, over email, instant messaging, or web meeting.

Content-Based Application Whitelisting

When an engineer uses an approved CAD tool to access a sensitive design file, that is very different from that same engineer accessing the same file using a web browser to upload the drawing to the Internet. With content-aware application whitelisting, you can create a whitelist of approved tools for specific classes for data (based on metadata, tags, or content inspection) or users. For example you can create a whitelist of approved engineering tools that engineers can use to access design drawings to ensure that data is being used correctly.

Application whitelisting works for both local executable applications and web-based or SaaS applications.

Content-Based Removable Device Whitelisting

Limit the type and model of removable devices that can be used by different classes of users , computers, or data. This allows you to require encrypted removable storage for IP or simply to prevent copying of certain files to removable USB, FireWire, or CD/DVD media.

Using built-in remediation workflow we automate data protection procedures such as encryption, logging, and manager approvals.

External IP Distribution Controls

Ensure that IP is shared with external partners or customers using the appropriate channel with the right level of data security. Global policies let you detect a data transfer initiated in email, FTP or instant messaging and:

Automatically route it to an approved secure channel such as a collaboration extranet

Automatically apply the right level of data protection such as encryption or digital rights management

Automatically initiate a remediation workflow, such as manager review and approval or export license determination.

Misdirected FTP or Email Distribution Detection

When IP is shared with external organizations over email or instant messaging, the product is able to compare the data being shared, such as a file attachment, with the recipient, in order to detect situations where the recipient is not associated with the same project as the data. An integrated remediation workflow alerts the user of the possible misdirection and allows him or her to correct the error by either changing the data they are sending or changing the recipient address. The users remediation actions are logged so that they can be reviewed by a manager or compliance officer.

Endpoint Data Loss Prevention

Endpoint data loss prevention (DLP) uses content analysis techniques to detect cases where sensitive IP is being leaked over endpoint ports and protocols including web uploads, file transfer, USB devices, writable CD or DVD, FireWire, and Bluetooth. Endpoint DLP can be used both for connected desktops and for offline laptops or laptops connected to public networks.

Mobile Data Encryption

When sensitive IP is downloaded to laptops or removable storage, policy can be used to automatically encrypt the files. The product supports three different models for encryption: built-in passphrase based encrypted archives, Microsoft Windows EFS (Encrypted File System) support, and integration with third party encryption tools such as PGP Desktop.

Just-in-Time Policy Education

In addition to enforcing policy, as seen in some of the applications described above, policy education can be delivered just-in-time. For example the Policy Education workflow can be used to notify a user when they have downloaded a sensitive document and highlight appropriate handling. Or, when a user copies a design drawing to a USB drive he can be reminded of the requirement to encrypt this data, and the encryption can then be performed automatically.

"Traditional security mechanisms no longer meet today's tougher demands for conducting business across an open, extended-enterprise environment. A new model is needed... Such a model would connect an organization and its business processes to all external stakeholders, seamlessly and securely, enabling employees, suppliers, and customers to collaborate anytime, anywhere, and at the lowest cost to all."1

Jerhico Fourm, The Open Group

1. "An Overview and How to Get Involved" by Jerhico Fourm, The Open Group., www.jerhicofourm.org

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS