



Achieving New Levels of IP Security

Most IP management solutions have put considerable energy into the former, but can you afford to put the right data into an insecure environment.

How important is information security for today's legal departments? According to research giant Gartner's Top 10 Strategic Technology Trends for 2015 "all roads to the digital future lead through security". When it comes to managing your IP portfolio, two fundamentals are paramount: the right data and a secure environment..

The worth of IP

In today's digital world, companies are moving toward a paperless existence in which IP exists almost exclusively in electronic files, databases and documents stored on servers. Obviously, the value of that IP goes way beyond the hardware and software used to store it, encompassing months and years of labor for development and marketing to create that value. Frequently information about business partners and other outside parties also are part of a company's IP store, and so recovery from a breach or data loss will often lead to penalties and liabilities that can quickly escalate.

How much of an issue is IP security? Increasingly staggering. Gen. Keith Alexander, former NSA chief and head of U.S. Cyber Command believes that the ongoing theft of U.S. intellectual property is "the greatest transfer of wealth in history." Furthermore, a 2014 study by Kaspersky Lab found nearly half of all ecommerce businesses and 41 percent of financial organizations reported losing data to cybercrime in the previous year thanks to malware, software glitches, theft of mobile devices and network intrusions to name just a few. And every market sector is vulnerable—a full 20 percent of manufacturers polled also suffered a loss of IP in the preceding 12 months.

The Commission on the Theft of American Intellectual Property estimated that US company revenue loss is now about equal to the total value of US exports to all of Asia, and the Center for Strategic and International Studies (CSIS), a Washington DC think-tank estimated the likely annual cost of cybercrime and economic espionage to the world economy at more than \$445 billion — nearly 1 percent of all income worldwide. "This is a global problem and we aren't doing enough to manage risk," said James A. Lewis, CSIS senior fellow and co-author of the July 2014 report commissioned by security firm McAfee.

The cost of even a single breach can be astronomic. Mizuho Investors Securities analyst Nobuo Kurahashi estimated the cost of Sony's recovery from the infamous 2014 data breaches to be approximately \$1.25 billion by the time the dust finally settles."

False sense of IP (and IT) security

The value of IP is dependent on its protection. And the purpose of an IP management system is to manage the processes and procedures related to protecting the IP. With up to 80 percent of a business' valuation bound in intangibles, corporations are motivated to operate in an open environment for maximum efficiency. Attorneys, inventors, marketers, and other stakeholders must share access to the IP data and documents in digital forms. But this open access creates an opportunity for misconduct.

In an effort to move toward an ever more open environment for processing IP from ideas to assets, many organizations are looking to leverage the Cloud. Rather than wasting precious time and money on a treadmill of constant hardware and software upgrades, smart IT organizations broker Cloud-based services and integrating those services into the existing IT infrastructure. They create and deploy most new IT services in the Cloud, and are increasingly looking at ways of migrating legacy and client-server applications to Cloud partners. But caveat emptor, as not all Clouds are created equal.

Location matters

Before addressing the differences among cloud solutions, let's first consider the risk of hosting the solution yourself. While some organizations still believe that securing IP and related transactions on-premises is the safest way to go, most have already moved to the cloud.

With respect to hosting the solution yourself, first there is the issue of aging infrastructure. Even now as Microsoft begins the rollout of Windows 10 in earnest, Windows XP still runs on millions of client PCs, and Windows Server 2003 on millions of servers. Unfortunately, these obsolete OS versions no longer receive ANY security patches or support from Microsoft, so any new vulnerability is easily exploited by hackers or malware writers looking to profit from the gaping security holes that these systems offer.

The nature of the threat landscape for IP has also evolved. Today's malware writers no longer act individually to create a virus or hack for notoriety, they are instead criminal enterprises with financial goals. Take the example of ransomware, which encrypts the contents of a server's storage—and only a payment to the hackers will provide the key needed to decrypt the data. What use is IP if it's inaccessible?

You are in the business of managing the law, not your systems. And I've met with hundreds of IP departments ranging in size from 1 to well over 100 members, none of them get the same level of attention from their IT organization as the sales and finance departments. Even the legal departments at the biggest software companies and tech giants struggle to get a tiny slice of the IT pie. In that environment, the legal department is always much better off with a managed hosted solution in which they are able to get automatic upgrades and have no responsibility for servers and server applications. Your IP is safer with a hosted IP management solution that offers the latest and greatest infrastructure, software, physical and logical security to ensure your IP's safety and your system's availability. Even some of the world's largest information security vendors utilize offsite IP management to ensure their IP value chain remains intact.

It is important to do your homework when choosing a hosted IP management solution. Your organization should have a good understanding of the proposed partner's security profile including both the application provider and the hosting services provider. Most IP management solution providers partner with a 3rd party to host the physical servers and access to the internet.

Four key security factors

Once the decision is made to utilize a cloud-based IP management solution, there are four critical factors to consider when evaluating possible partners to ensure a successful implementation.

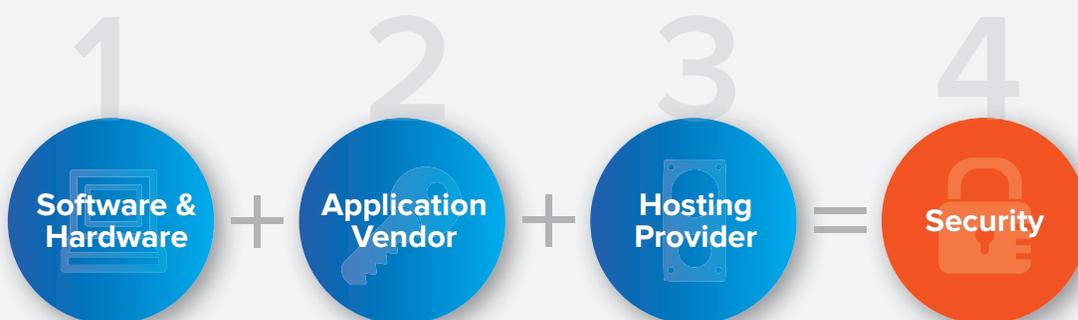
First and foremost, ensure that the provider you choose is up to the task. Look for providers offering a solid track record with a tested and audited solution. And since solutions often incorporate both hosting provider and application provider, ensure your chosen partner can produce certification from auditors that demonstrate both application provider and hosting provider (if different) are dedicated to security. Without that level of security and auditability, your IP management provider may be the weakest link in your security and privacy chain.

Second, ease the internal IT burden by federating identity so users need only provide a single sign-on (SSO) for all applications, including IP management. This serves multiple critical functions. First, it allows the use of a single, trusted identity source such as an internal Active Directory or other trusted directory. SSO solutions may also provide their own authentication or utilize other social services to authenticate users. More importantly, strong authentication strengthens IP security overall, as over two thirds corporate IP theft occurs from within an organization. Knowing who accessed what—and when—provides an audit trail that can help prevent a theft before it happens.

Third, look both ways—inside and out. Insiders can present a greater risk than outside threats, since in many cases insiders use authorized access—or did not even require authorization—to pilfer IP. As you firm up your IP security plan make sure your provider offers the kind of audit trail that will let you know who accessed IP for any reason at all, or better yet ensure your provider enables role-based authentication and access that prevents most insider theft before it can happen.

Finally, once you have established your secure IP management environment, use it! The best way to maximize adoption of the new system is to begin with the end in mind. Include representatives from all stakeholders in the process from the beginning. Select a system that is both secure and flexible enough to meet the needs of your unique organization. Involve them in the deployment of the system and train all users thoroughly in both the use and advantages of the new system. If you skip any of these steps, you face the risk of users tempted to bypass a new IP management system, and all of your efforts at security are wasted. Today, most organizations still send data to their outside law firms and trust that it is safe and secure there. However, we should be moving toward a goal of a single system of record for all high security data that is accessible only by the right parties at the necessary stages in the lifecycle of the IP.

FOUR KEY SECURITY FACTORS



The security of the information in your IP management system is dependent on this equation. If any component is 0, then the whole system is compromised.

What's next

Ready to accelerate your IP value chain while improving IP security? Only one IP management solution has been audited and certified from end-to-end—just as the hosting companies have been—to ensure that your IP is secured with the highest levels of physical and logical security available. Lecorpio, the leader in IP management, now has the same SOC-2 compliance that major hosting companies ascribe to, thus offering you an enhanced security environment that is unmatched by any other IP management provider worldwide. To find out how you can get the most out of your IP while ensuring the highest levels of security and compliance for your organization just surf over to www.lecorpio.com to and out how to get started.

About Lecorpio

Lecorpio, the leader in IP management and analytics solutions, helps innovative companies quickly turn ideas into assets. The enterprise-class suite of applications spans the entire IP supply chain, including invention disclosure management, patent and trademark management, e-billing, licensing management and general matters management. The solution includes powerful work flow capabilities that easily configure to a company's business process and includes an IP dashboard with over 160 KPIs.

Lecorpio is used by 5 of the top 20 most active US patent filers, as well as well-known innovators such as Adobe, T-Mobile, Analog Devices, Rockwell Automation, NEC, NetApp and Red Hat.

More products from Lecorpio

Lecorpio offers a full suite of products that can be combined to deliver the perfect solution to empower your IP department.

Simply click on one of the products sheets to instantly download.
(must be currently online for access).

[Invention Disclosure Management](#)

[Patent Management](#)

[Annuity Management](#)

[General Matter Management](#)

[Trademark Management](#)

[Spend Management](#)