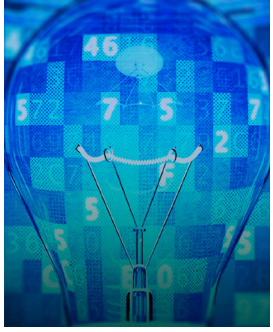

The Security Imperative: 9 Key Questions to Answer Before Implementing IP Management

Your Intellectual Property is mission-critical, and protecting it with enterprise-class security is paramount. That said, many companies deploy less-than-optimal solutions because they haven't carefully considered these important questions before making a decision:

1 How is my data stored?

There are two ways to store data with an IP management solution: 1) On a hosted infrastructure — also called cloud, or Software as a Service (SaaS); or 2) On premise, where you manage the IT infrastructure necessary for deployment. The assumption many make is that by running the infrastructure themselves the environment is naturally more secure. Control, however, is not synonymous with better security. In fact, cloud-based service providers often spend far more on security than enterprises because their livelihood depends on providing a secure environment to their customers.

A 2012 study from Alert Logic discovered that on-premise environments were 12 times more likely to have security configuration issues which increases the risk of becoming compromised. Internal IT departments must be committed to providing the same level of dedication to security as cloud-based providers, with highly controlled access, proper configuration, and 24x7 monitoring. In the end, it comes down to weighing the trade off between the perceived benefits of total control versus the real incremental cost of deploying internal resources necessary to ensure bullet-proof data security.

2 Is the hosted model single-tenant or multi-tenant?

In a hosted, cloud-based model, there are two ways to store data. The first is single tenant, an architecture in which a single instance of the software and supporting infrastructure serves one customer. With single tenant, an organization's data remains separate from the data of other companies using the same solution.

Multi-tenant is an architecture where a single instance of the software serves many customers. With multi-tenant, an organization's data can't be viewed by others using the system, but it is stored with other users' data.

Multi-tenant is more economical because a provider only has to update one instance of the software. A multi-tenant solution, however, lacks the security of a single-tenant solution. Organizations that require higher levels of security for their IP will want to consider a single-tenant solution.

3 How is my data protected?

Encryption is the process of encoding data so that only authorized people can read it. While encryption does not prevent hacking, it does make it more difficult for the data to be read by an unauthorized person. There are two types of encryption that should be used to protect your data:

- **Encryption in transit:** Data is encrypted as it is shared between two users so that if someone were to intercept the message in transit, they could not read it.
- **Encryption at rest:** In addition to encrypting data that is being transmitted, data should also be protected where it is stored in case of unauthorized access or theft.

4 What steps are taken to physically secure my data?

In addition to cyber security, you must also consider the physical security of the data center where your data will be stored. Keep in mind these three considerations:

- Providers should not reveal the location of their data centers.
- The perimeter of the data center should be secured using access controls, and the front of the building should have barriers to prevent vehicles from attacking the structure.
- In addition to video surveillance throughout the entire data center, servers should be protected with biometrics at no fewer than three separate points of access.

5 What is your disaster recovery strategy in case of catastrophe?

Data protection must not only include prevention of malicious activity, but also unforeseen disasters such as floods and fire. Those responsible for IP management at their organizations will want to ensure their solution has a fail-over mechanism that limits downtime in the event of a disaster.

For a hosted solution, this will include using a cloud-based model that ensures high availability. By leveraging the cloud, multiple copies of your data are stored in various locations.

For on-premise, you will want to mirror the data at a separate facility that is geographically distant from your enterprise. The cost is high, but that's the only way you can ensure protection from disasters and unplanned outages if your system is located on-premise.

6 How often will my data be backed up and how are the backupsprotected?

Backups take a snapshot of your data and store it in case something were to happen. Your data is mission-critical so regular data backup is imperative (sometimes as frequently as daily, but weekly is the typical best practice). Additionally, you should have several redundant backups that extend for multiple periods. Why? Because this is the only way to ensure you can quickly return to full production should a disaster occur. Again, for on-premise models, these backups must be stored at a separate facility that is not closein proximity and should have the same encryption and physical security measures put in place.

7 What browsers, operating systems, and devices does the software support?

Sophisticated IP management environments will include many different people, both internal and external to your organization. Given this, there will be many different ways users will want to access the data. To ensure high availability to all users, the IP management environment should be browser, operating system, and device agnostic. Make sure your software solution doesn't limit what browsers and operating systems it supports, and check that it can provide users access through mobile devices such as tablets and smartphones.

8 What happens to my data if you cancel your subscription to the software?

If you decide to switch vendors, it is crucial that you own your data and have uninterrupted and unlimited access to it. You should not have to pay to get special access to your data.

Before implementing any IP management solution, be sure to ask your prospective provider what happens to the data if you cancel your subscription to the software. There should not be any special fees or switching costs associated with the transfer. After all, it's your data.

9 How are intrusions into the data detected and prevented?

Intrusion detection and prevention systems (IDPS) monitor network traffic for malicious activity. They provide event-log analytics to detect insider threats, inspect security configurations, and ensure file integrity. Every time someone requests data, the traffic should ow through an IDPS. No exceptions! Once malicious activity is detected, the system should send an alert to the administrator and block traffic coming from the intruder's IP address.

In addition to continuously monitoring network traffic with an IDPS, organizations should also conduct regular audits: quarterly "black box testing" to ensure the system is working properly, and annual "white box testing" to identify potential security risks and implement security measures to mitigate vulnerabilities.

IP Management Solution Security Checklist

To determine how secure your IP is today, answer the following questions.

Each "Yes" response increases the security of your IP management solution and the availability of your data.

1 Is the data stored in the cloud?

☐ Yes ☐ No

2 Does the vendor encrypt the data in transit?

☐ Yes ☐ No

3 Does the vendor keep the location of the data center a secret?

☐ Yes ☐ No

4 Is there video surveillance installed throughout the entire data center?

☐ Yes ☐ No

5 Does the vendor protect your data from unforeseen events such as disasters and acts of God?

a. Fail-over mechanism that limits downtime

☐ Yes ☐ No

b. High-availability architecture

☐ Yes ☐ No

c. Mirrored data at a separate facility that is geographically distant from the other data center

☐ Yes ☐ No

6 What browsers does the host support?

a. Chrome

☐ Yes ☐ No

b. Internet Explorer

☐ Yes ☐ No

c. Firefox

☐ Yes ☐ No

d. Safari

☐ Yes ☐ No

7 If you cancel your subscription do you have access to your data without paying a special transfer fee or switching cost?

☐ Yes ☐ No

8 Does the vendor conduct regular audits including "white box testing" and "black box testing?"

☐ Yes ☐ No

9 Is the data stored in a single-tenant architecture?

☐ Yes ☐ No

10 Does the vendor encrypt the data at rest?

☐ Yes ☐ No

11 Is the perimeter of the data center secured with access controls and physical barriers at the front of the building?

☐ Yes ☐ No

12 Are the servers in the data center protected with biometrics at three or more separate points of access?

☐ Yes ☐ No

13 Will the data be backed up daily?

☐ Yes ☐ No

14 Can data be accessed from smartphones and tablets?

☐ Yes ☐ No

15 Does the vendor deploy intrusion detection and prevention systems (IDPS) which monitors all network traffic?

☐ Yes ☐ No

For more information on how Lecorpio answers these questions, visit www.lecorpio.com.

Lecorpio's enterprise-class suite of pre-built applications spans the entire IP supply chain:

Lecorpio Invention Disclosure Management

Lecorpio Patent Management

Lecorpio Annuity Management

Lecorpio Trademark Management

Lecorpio General Matters Management

Lecorpio Spend Management

"Rather than telling us the way things had to be implemented, Lecorpio's team listened to what we needed and made suggestions about our different options."

Joseph Kolodka
Lead Counsel
IDM NEC Labs

Lecorpio helps the most innovative companies turn ideas into assets via work flow, data insights and portfolio management.

Orchestrate Produce higher quality IP faster by establishing a defined work flow.

Analyze With Lecorpio, you can assign the right task to the right person at the right time.

Optimize Gain critical insight into the key metrics and data that are affecting innovation across your organization.

Elevate Simplify and automate IP processes to control costs and increase efficiency. Maximize the value of your IP through effective IP portfolio management.

Learn more about Lecorpio's enterprise-class suite of applications
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