In an era of increasing data theft, it is important for organizations to ensure that the Intellectual Property related to their offshore outsourced projects stay safe. Here is a roadmap that can help you address this concern.

Aviraj Jain
INTRODUCTION

Protecting Intellectual Property (IP) is essential for organizations willing to sustain their competitive edge. The need to protect IP becomes even more critical in offshore outsourcing since it involves sharing a wide array of intellectual assets.

The Data Breach Investigations Report (2013) by Verizon reveals that attackers are interested in all kinds of IP, including customer lists, designs, product roadmaps and code. Several other global research findings also confirm that IP-related attacks are increasing in frequency and sophistication with every passing day.

Therefore, the fast evolving IP theft landscape calls organizations to be prepared with stringent IP protection measures. Offshore outsourcing calls for a comprehensive IP protection framework. This exercise begins with selecting an offshore outsourcing partner, based on its IP protection capabilities. Outsourcing organizations will need to assess the quality assurance and security management standards of the partner (e.g. ISO/BS or CMM certifications). They will also need to examine the legal framework of the potential partner’s country.

The other aspects of IP protection that offshore outsourcing organizations will need to evaluate are related to the contractual terms.

However, even while you employ a well-thought strategy, there is no magic bullet to ensure complete protection against IP theft. The best you can do is to adhere to a proven set of guidelines that will help you mitigate IP-related risks. This white paper describes these guidelines that encompass legal, physical, logical, procedural and managerial aspects of IP protection.
ESSENTIAL STEPS TO PROTECT IP

Once you finalize your offshore outsourcing partners, ensure that they adhere to the following crucial aspects of IP security:

1. Identify the IP Inventory that is to be Outsourced
2. Nominate Persons at both ends - Customer and Vendor - Responsible for IP Security
3. Fix the IP Location
4. Put Legal Framework, Checks and Controls
5. Do Regular Checks and Audit

GUIDELINES FOR PROTECTING IP WHILE OFFSHORE OUTSOURCING

The broad set of guidelines that your organization will have to follow while offshore outsourcing is listed out in Figure-2.
DETERMINE CONTRACTUAL & CONFIDENTIALITY AGREEMENTS

Following are the aspects related to contractual and confidentiality agreements that you will need to ascertain:

- **A Formal Contract:** A formal contract must exist between you, the customer, and the vendor to protect both parties.

- **A Confidentiality Agreement:** A binding confidentiality agreement should be signed between you and the vendor, either as a part of the contract itself or as a separate Non-Disclosure Agreement (NDA).

- **Clauses to Retain IP Ownership Rights:** The contract must have a clause to empower you to retain all ownership rights over their IP assets.

- **Clauses to Secure Confidential Information:** The contract must hold a clause for securing confidential information.

- **An Information Classification Policy:** According to Information Classification policy, all information must be controlled and classified.

- **Indemnification Provisions Addressing IP Breaches:** In order to address IP breaches, the contract must include provisions of indemnification. This can protect your organization from the potential risks of IP breaches.

- **Sufficient Insurance Coverage:** The vendor should ensure adequate insurance coverage to protect itself against all claims and liabilities arising from its performance under the Agreement.

- **Information Security Obligations and Control Details:** The contract must include references to Information Security obligations and controls, such as, Information Security policies, procedures, standards & guidelines.

Figure-3
ENSURE PROPER HIRING & TRAINING OF EMPLOYEES

You will need to ensure the following:

- Check the Background of Employees: Employees working on your behalf at the vendor-end should be subjected to background checks.

- Provide Training and Education on Information Security: Employees working on the contract should be provided with training and education on information security.

PLACE ACCESS CONTROLS

Ensure robust access control architecture, to prevent unauthorized access to your information assets by the vendor.

- Physical Access Controls, including:
  - Layered controls covering perimeter and internal barriers
  - Suitable locks with key management procedures
  - Access logging through the use of automated key cards, visitor registers, etc.
  - Users defined user roles with appropriate logical access rights and controls
  - Data encryption in accordance with customer’s encryption policies
  - Intruder alarms/alerts and response procedures

- Separation of the Customer’s Assets from Other Systems:
  - If your IT infrastructure is hosted at a third party data center, your assets should be physically and logically isolated from other systems.

- Separate VLAN's for the Project:
  - Separate VLANs should be created for the project and proper inter VLAN securities should be enforced.

- Technical Access Controls, including:
  - User’s identification and authentication

- Authorization of access generally through assigning standards
- Defining Algorithms, key lengths, key management, escrow, etc.
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations wherever applicable

- Information Assets Management & Restricted Internet Access:
  - Proper management of information assets should be ensured. This can be accomplished by duly retrieving or destroying them. Restricting internet access is also advised.

- Vulnerability Assessment and Penetration Testing (VAPT):
  - Internal and external VAPT should be carried out on a periodic basis to fill up security gaps, if any.

- Access Controls Documentation:
  - Proper documentation of procedural components of access controls should be ensured within procedures, guidelines and related documents.
ENSURE STORAGE PROTECTION
Effective data leakage prevention initiative begins with protecting data at its repository (IDC, 2011). Ensure that the place where your data is stored is well-protected.

IMPLEMENT SYSTEMIC CONTROLS
Ensure that your vendor has placed suitable system controls to protect critical information, such as IP and Personally Identifiable Information (PII), such as, name, address, phone numbers, etc.

UNDERTAKE SECURITY AUDIT
As a procedure you must audit your vendor’s premises at regular intervals, to ensure that vendors are consistently complying with requisite security policies and your IP protection requirements.

CONCLUSION
Effective IP protection is of utmost significance for businesses. In offshore outsourcing arrangements, both the customer and the vendor need to strictly implement an appropriate set of security controls to reduce IP-related risks. This is possible when both parties collaborate to device a robust security framework and ensure that they stringently adhere to it. A comprehensive management of IP-related risks will ensure that your organization will be able to sustain its competiveness and derive optimal value from the offshoring arrangement.
ABOUT THE AUTHOR:

Avirag Jain has 25+ years of rich experience in the IT industry including managing large on-site, off-site and offshore projects. He currently heads the Offshore Development Center of R Systems International Ltd. as CTO and EVP. Avirag is a science graduate with PGD in Cyber Law. He also holds an MBA degree with specialization in Finance and International business.

Email: avirag.jain@rsystems.com / jain.avirag@gmail.com

ABOUT R SYSTEMS

R Systems is a leading OPD and IT Services company, which caters to Fortune 1000, Government, and Mid-sized organizations, worldwide. The company is hailed as an industry leader with some of the world’s highest quality standards, including SEI CMMI Level 5, PCMM Level 5, ISO 9001:2008, and ISO 27001:2005 certifications. With a rich legacy spread over two decades, we generate value that helps organizations transcend to higher levels of efficiency and growth.

For more information, visit www.rsystems.com