Software Development Offshore Outsourcing: Protecting IP

A White Paper by Jack Olson

August, 2014
Austin, Texas

Concerns for IP protection when using offshore outsourcing for software development always becomes an important issue. As well it should. The concerns are not different from those that face any software development company whether they use offshore development teams or not. For some reason there is a belief that offshore programmers are more likely to violate IP rules than onshore programmers. History does not support that contention.

Fears

The fears most often heard are:

1. They will steal the entire product and offer it for sale in their own country or others.
2. They will sell the entire source code for a product to a competitor.
3. They will use components of your code in other projects they are working on for other clients.
4. They will use components of other clients code in your products.
5. They will use open source code in your product that should not be used.
6. They will put some of your code into open source.

These fears are all relevant and most, if not all, have occurred through offshore outsourcing projects. Most, if not all, have also occurred through in-house programming teams at home. In my personal experience I have seen or heard of offshore teams doing items 3, 4, 5, and 6. I have personal knowledge of onshore, in-house teams doing 4, 5, and 6. I have also personal knowledge of non-programmers employees of software companies in foreign subsidiaries doing items 1 and 3.

My own experience tells me that the risk of using offshore outsourcing teams is no higher than using at home programming teams:

	Offshore Programmers	**In-House Programmers**	**Offshore Non-Programmers**
1. Steal your product			
2. Sell your code			

3. Resell your components			
4. Resell others' components			
5. Misuse open source			
6. Open source your code			

Likelihood of Occurring

The likelihood of violations occurring is not high. The offshore programmers value their jobs more than programmers at home. They have fewer alternatives and are paid more than other programmers in their country doing work for local companies. These countries have an excess of trained programmers and thus finding an equivalent or better job is more difficult. Putting their job at risk makes no sense. The same is true for the outsourcing company. They worked hard to build up business and they know that a single violation could put them out of business based on an earned bad reputation.

> Note. It is worth nothing that the demand for programmers in those countries is recently higher and growing. The “coopetition” among HR makes those facts immediately known; such a violator incurs a real risk of going out of profession.

It is also true that the likelihood of violations is much higher if the client does not take steps to educate the outsourcing programmers, establish a secure development environment, and diligently monitor for violations. If people understand what they are supposed to do and not do and if they are made aware that they will likely get caught if they break the rules, then they will almost always behave responsibly.

Redress for Violations

When violations do occur, the client is at a disadvantage if seeking redress. The client can always fire the outsourcing company or at least fire the programmer that exhibited the bad behavior. However, seeking financial compensation for security breaches becomes problematic when it requires filing a lawsuit in the outsourcer’s country. If you succeed, the cost of legal representation would be large. The time to do so would also be very long. Getting stays for violating products would also be

difficult to get or enforce. The probability of any suit being successful would be less than 5%. If successful, the guilty would, in all likelihood not pay the redress since they rarely have deep, or even shallow, pockets.

Some redress can be achieved when the outsourcer has a local office doing business in the client's country. In this case a local suit can be filed and would generally succeed. You can also sue any company selling a software product in your home country that contains code stolen from your development efforts . This also applies to other countries where the offending product is being sold and where you can find a reasonable legal environment to seek compensation.

This is a big advantage to the client since few software products have meaningful markets in outsourcing countries.

A Strategy for Outsourcing Activities

The best approach is to address the topic head on and do everything possible to build a secure environment and prevent the violations from occurring in the first place. The strategy should include:

1. Avoid tempting opportunities.
2. Strong terms in the contract with the outsourcing company.
3. Education of the outsourcing team members on their responsibilities and consequences of violations.
4. Establishment of a secure development environment.
5. Diligent monitoring of all development activity.
6. Detailed record keeping.

Avoid Tempting Opportunities

One of the most obvious measures is to not select an outsourcing company being used by a competitor. This sounds obvious but few companies actually check this. You should always be aware of what companies are using the same outsourcer you plan to use especially at the same development center.

Also, make sure that you have filed patents on your inventions as early as possible and, if possible, before the outsourcer knows about that part of a project. Make sure your outsourcers know about your patent applications and understand the implications of violating them.

As a special note on the topic of patents, if an outsource team invents something that can be patented, you should file the patent with them listed as the inventors if possible (depending on local laws) with your company as the owner of the patent. Your contract should explicitly indicate that any inventions belong to you and not the programmer or the outsource company. This is not only proper, it gives the outsourcer an added incentive to protect IP.

Another way to eliminate temptation is to not give the outsourcer the job of developing an entire product or the ability to bring together an entire product for testing. This involves having a second development team, either at home or through a different outsourcer or both. The outsourcer is unable to acquire the entire product and therefor is not likely to rip off a meaningful collection of code.

Contract Terms

Everything starts with the contract between the client and the offshore outsourcing company. The best practice is to develop a single contract between you and the outsourcer that spells out how everything will work for projects. Individual projects will be described as attachments to this contract and will all inherit the same contract rules. One lasting contract.

The parts of the contract that relate to IP protection should include expectations of the outsourcer, responsibilities of the outsourcer, steps expected to be taken by both parties, and documentation that is to be created and retained by both parties. In short it should include wording to cover virtually everything covered in the rest of this paper.

It should cover the process used to add anyone to the team. This should include documents to be signed for non-disclosure, assignment of rights to all code developed to the client, assignment of all inventions made to the client and attendance at a class on protection of IP rights.

The contract should state the client's rights to take punitive action in cases of IP security violations. This should be non-negotiable. The right to have someone fired without recourse must be in the contract. It should also state the process used

to fire a person: documents to be signed by fired employee, all materials to be returned, employee walked out the door, return of space entry cards/keys, etc.

The contract should specify that the entire relationship can be dissolved immediately for IP violations as well as other violations of law. The contract should also have a clause to allow termination for any reason on 30 days' notice by either party.

The contract may indicate a process for arbitration of such instances. If so, it should state the location of the arbitration as in the client's country and state that the client selects the arbitrator.

The contract terms should be reviewed at least annually with changes made as appropriate. It should be reviewed by your legal team, if not created by them.

Education of Offshore Staff

The contract should require that every employee of the provider that will be working on the projects be identified in writing to the client. This includes management and administrative staff as appropriate. The contract should specifically state that others should not be used on the project or exposed to any information about the projects. It should specifically disallow "back-door outsourcing". If back-door outsourcing is required then it the back-door outsourcing company should be placed under contract with the client and follow all the same rules.

Each employee should sign a non-disclosure agreement and an employee agreement. The employee agreement should specifically address the need to protect intellectual property with MUST NOT DO items. For example, they should not use code developed for other clients, they should not use code developed for this client in other projects, they should not use open-source code without prior approval, etc.

It is important that the employment agreements signed by the individual programmers state clearly that all code developed is the property of the client. It should indicate that the programmer automatically surrenders any right to the code by signing the agreement. Many countries have a law that gives programmers ownership rights to any code they write no matter who they write it for. In all cases, the employment agreement should clearly state that by receiving compensation, they give up this right.

It is not acceptable for the outsourcing company to agree with this but not get agreements with each individual programmer. Many contracts call for this and other documentation to be signed only by an officer of the outsourcing company. Although this may have legal standing, it fails to get the individual employee involved in understanding and agreeing to security terms.

If the country of the outsourcer does not automatically assign ownership to the programmer, it does not hurt to get the agreement signed anyway. Although it would be moot by law, it is a good way to remind the programmer of the terms.

Each employee should be required to attend a 1 hour IP protection class. They should sign a document at the end saying they attended the class and understand the content. The class should be conducted in the language of the provider or have a translator present to ensure understanding.

All of these documents should be written in two languages: the language of the client and the individual.

Establishing a Secure Development Environment

You must recognize that an outsourcer has other clients. It is to their advantage to house all projects in one place and have everyone have access to this single place. It makes no sense for you to go to lengths to get each programmer working on your project to sign security document is they work in the same space as programmers who have not signed them. If your projects require security then you should take steps to secure the working space just as you would at home.

I have seen, and used, practices of having projects isolated to a specific floor of a building with key-card access provided to only project members. I have also seen forced (by contract) separation between buildings and even cities. In no case should programmers not assigned to your project have access to the space used by your project. This requirement may cause the outsourcing company to spend more money but, in the long term, the amount will not be much.

Code Protection

The working environment should utilize a source code control system that protects all code developed from being seen or copied by unauthorized people. The programmers should use only this system to develop code.

The system should allow for a mirrored repository of source code that will be put on a server in the USA or in the cloud. This repository should sync with the work being

done by the developers on a daily basis. Note that the client's version of the source code libraries may contain source code from multiple development sites, not just the one outsourcer. If so, the outsourcer's programmers should not have visibility to the code they do not develop or need.

All transfer of data between outsourcer servers and client servers should be encrypted.

The source code management system should allow for automatic inclusion of copyright comments and variables in all source code modules.

Documentation
All design documentation and user documentation should be clearly marked as Confidential property of the client.

Wiki sites should be password protected.

Emails
It is recommended that the project team members use the client's email system for all project communications. Emails should not be sent to or from the outsourcer programmers personal email addresses.

Test Data
If you have test data for quality assurance and this data has sensitive information in it that must be protected, then ensure the outsource team is properly educated on what needs to be done. In general, you would not expose real world data to an outsourcer's quality assurance team. If necessary consider using data masking technology to generate test data that is not sensitive.

Monitoring Development Activities

The client should have someone on his staff assigned to a project management role and a technical leadership role. In addition to their other duties, they should be responsible for monitoring all offshore outsourcing development activities for security purposes.

The technical person should periodically check source code for proper copyright statements, comments that may indicate that code was brought into the project from other client's projects, and open source usage.

Open source usage should be approved before used. All open source packages have an implied contract for use. Some of these are inappropriate for use in commercial software packages. For example, they may require any product that uses the code to be put into open source. Before an open source package is used, the contract terms for use must be reviewed and approved by client management. The technical leader at the client's staff must ensure that only reviewed and approved open source be used.

The technical leader should be constantly reviewing the source code being developed for other reasons besides security.

The project leader should ensure that all rules for hiring or firing outsourcer employees be followed to the letter. He should be responsible for ensuring that site security is established and followed as needed.

I recommend that both of these individuals make periodic visits to the outsourcer's development sites to ensure that rules are being followed and to continually remind the outsourcing team that you are serious about them. When making visits, look for programmers you do not know. If you find one, challenge the outsourcer's management on who they are and whether they have been properly brought on board to the project.

Record Keeping

All documents regarding security should be kept at the client's site. This includes contracts, employee agreements, employee non-disclosures, employee assignment documents, records of security classes held, and records of when visits are made, source code is reviewed, and anything else you do.

All documents from the outsourcer team should be signed by individual programmers where appropriate and also by an officer of the outsourcing company.

Your paper trail should document that you took every measure to protect your intellectual property and that you diligently monitored development activity to ensure compliance.

This is not a lot of record keeping and, once implemented will become automatic. It can only pay off in the end. If your outsource company knows you are going to these lengths to protect intellectual property they will take it more seriously themselves.

Final Thoughts

In the end protecting your intellectual property is a matter of risk. Anytime you expose your intellectual property to anyone whether in an offshore company or at home in your own staff, you are taking a risk that they will violate your trust. The more you educate them on what is expected and what the consequences of non-compliance will be the higher the probability that they will do what's right.

If you have sound security measures and can document that you diligently followed all of them all of the time, you are in the best position to seek redress if a violation occurs. You will also probably discover any violations earlier. Although it's true that achieving redress is difficult, if you take steps to reduce the risk you should not need to deal with this.