Securing Outsourced Projects

By: Rajesh Pandey

You outsourced your application development to save money, right? Or perhaps you did it to temporarily scale your development capacity to tackle a special project. It makes sense for organizations to outsource development in these situations. However, you can bet the streamlined, highly optimized software factory that you have hired to do your development is not putting security at the top of its priority list.

Security is an emergent quality of an application; it is not something that you automatically include by selecting a certain technology, process, or language.

Within one application development project is a complex system made up of many technologies, platforms, configurations, and programming styles that you expect to behave the way you designed it to. If you made missteps at any point and did not properly address the security of your design, code, and configurations, then you probably have introduced security vulnerabilities into your application.

When you outsource development to someone else, you have to trust that they are properly accounting for the security risk of your application. So, how are you measuring the success of your outsourcer? Most likely you are measuring--maybe even compensating--your outsourcer's ability to meet deadlines, adhere to budgets, and meet minimum quality criteria. But does your contract include security testing? Does your outsourcer's warranty address its liability if a severe security vulnerability is discovered in the production system? To be sure that your outsourced application is secure, you should require that security be a priority to the outsourcer, on par with cost and quality.

Require Security Standards throughout the Software Development Lifecycle

The only way that your outsourcer can dependably produce secure software is by addressing security issues properly throughout the software development lifecycle. Whatever process it has chosen to follow is probably not much of a concern to you, but you need to be sure that security

touches every part of it.

Ask to see the secure coding standards the outsourcer follows. Find out what kind of security training is given to its developers. If you are hiring the outsourcer because it might know more about software development than you, then you should certainly expect that it knows more about software security than you. Make sure the outsourcer is at least addressing the security issues listed in the Open Web Application Security Process (OWASP) Top Ten. Find out if it uses any security vulnerability assessment products. Make the outsourcer demonstrate its security knowledge to you by showing evidence of it throughout the process.

Mandate Security Testing

Only by testing an application can you be sure that the best requirements and designs were implemented properly. At the same time, you can only be sure an application is secure if it is tested for security.

No matter how much your outsourcer's developers know about security and no matter how closely they adhere to security best practices, they need to prove to you that they have tested their code and can assure it's safe.

Require Security Audits as Application Acceptance Criteria

In a services relationship, such as the one between you and your outsourcer, your vendor will work to maximize its performance in the areas you measure. In other words, if your contract sets timelines and cost targets, your outsourcer will do everything to meet the dates and keep the costs in line. If you mandate certain quality levels, such as "no Severity 1 defects," then your outsourcer will focus on fixing the defects required to get the system to an acceptable level of quality.

You should always require that your outsourcer conduct security audits of the application that it delivers to you using your accepted minimum level of security risk in the system. For best results, you should mandate the use of a third-party security auditor that has the expertise, experience, and tools required to accurately assess your application's security risk. Ultimately you must determine the minimum security risk you are willing to live with and accept nothing more.

USA	India		
Corporate Office	**Development Center**	**Regional Offices**	
7 Lincoln Highway, Suite 205, Edison, **NJ** 08820 Phone 732.548.9268 Fax 732.548.8913	Plot No. 38, Electronics city Sector 18, **Gurgaon**-122 015, India Phone: 91-124- 2397660-62, 5017660 Fax: 91-124- 2397655, 5019955 http://www.binarysemantics.com	20, 2nd Floor, Arihanth Complex 1st Cross, CKC Garden (Off: Mission Road) **Bangalore** - 560 027 Phone: 91-80- 22240222 / 22241222 Fax: 91-80- 22277867	Basera - Plot No.48, 3rd Floor, Santhawadi Lane Opp. Jain Upasarai, Jaiprakash Road, Andheri (W) **Mumbai** - 400 058 Phone: 91-22- 26705762 /26286748/62 TeleFax: 91-22-26705763