

# Security threats offshore

## PROTECTING INTELLECTUAL PROPERTY REQUIRES VIGILANT NEW POLICIES

Exclusive for San Jose Mercury News

By Rahul Sood

The media have recently attributed several cases of intellectual property loss and privacy violation to the outsourcing of work to foreign countries. This has added to the controversy surrounding the growing number of U.S. companies turning to cheaper labor overseas.

There are a variety of reasons why offshore labor is unpopular right now. However, security concerns should not be one of them. Most U.S. companies using offshore labor should be able to prevent security issues by taking some precautions.

The security risks to intellectual property are mainly driven by two factors. First, laws protecting intellectual property are not as stringent abroad as in the United States. Second, employees are the most common source of security breaches, and when companies hire contract workers in foreign countries, they bring on a large number of virtual employees over whom they have little control.

The risk of losing valuable data through foreign contract workers is real, but it can be diminished through a combination of practices, policies and contractual arrangements.

Here are three areas that can ensure greater security when American companies use offshore labor:

**DEMAND "SAFE" HUMAN RESOURCES PRACTICES** -- Look for vendors whose security processes are certified by independent third parties. Do background checks of employees during recruitment. Non-disclosure agreements with employees and frequent training on security procedures are critical.

Investigate offshore vendors' internal processes. Install management software that provides visibility into who is working on tasks. Conduct surprise audits of offshore operations to ensure compliance. Ask for "non-compete" clauses that prevent select contract workers with access to confidential information from working for competitors for 6 to 12 months.

**KEEP CONTROL OF TECHNOLOGY POLICIES** -- To prevent unauthorized workers from gaining access to sensitive data, prohibit farming out work to sub-contractors. The outsourcing of information technology work to foreign countries should include additional protection such as banning Internet access at employee work stations, restricting access to printers and keeping control of firewall and network security settings.

**CREATE LEGAL AND CONTRACTUAL DETERRENTS** -- U.S. companies should ensure that contracts with foreign workers are under U.S. jurisdiction as well as being enforceable in the workers' country because different countries have different levels of laws protecting intellectual property. It's essential to work with lawyers who are experts in contract law in the United States and the country where work is being sent. Determine upfront what intellectual property is owned by the customer and what is contributed by the offshore vendor; that way, everyone involved will be protected.

Will we see more security breaches? Unfortunately, yes. There are thousands of offshore vendors serving U.S. customers. Not all vendors have the same standards nor are they in countries with equal levels of legal protection for intellectual property. U.S. companies that choose to use offshore labor ultimately retain responsibility for their own security.

Despite the attraction of lower wages, offshore labor presents numerous challenges. They can be underestimated, but most can be managed.

One long-term answer to the problems of security in sending work offshore is that overseas vendors

need to take the lead in establishing industry standards. They have an obligation to lobby their governments to strengthen domestic intellectual property laws.

RAHUL SOOD is a principal at Tech Strategy Partners, a Redwood City-based consulting firm that advises software companies on offshoring. This column was written for the Mercury News.