

DEPARTMENTS

news

November 2003

GOING EAST

Bargain-hunting companies look off shore for programming, but at what cost?

BY ERIK SHERMAN

Horace Greeley told people to go West for their fortunes, but corporations are looking east--the Far East--to save money on software development.

Instead of paying programmers handsome annual salaries and benefits, companies are finding trained and hungry experts overseas. For a fraction of the domestic costs, businesses such as Oracle and Guardian Insurance are getting coding for products or internal applications in India, China, Russia and elsewhere.

The results work well enough that the practice has expanded. But specters of cyberterrorism, computer crime and economic espionage make application integrity and security major issues. Those safely succeeding are finding that they must rigorously choose their offshore partners, perform extended due diligence, set clear expectations, create a legal framework, and stay thoroughly involved in the process to remain safe.



There are two potential problems when someone--an employee or third party, foreign or domestic--writes code for a company: the inclusion of malicious code--logic bombs, sniffers or backdoors--or coding mistakes and poor coding practices that leave software vulnerable to exploitation.

"The big concern is that whoever [a company] contracts with will look at security control at the same level as the company itself," says Al Marcella, an associate professor of management at Webster University in St. Louis, and a veteran of numerous security audits. "If a corporate headquarters has policies of background or security checks, is the third-party provider doing the same quality, level and type of check?"

Although malcode might receive the most public attention, coding errors are the greater problem. Most recent security flaws were caused by man-made error, says Marty Lindner, team leader for incident handling at the Carnegie Mellon's [CERT Co-ordination Center](#). "Code is continually being produced that has a small number of well-understood programming flaws," he says. "It was [due to] the lack of due diligence of the programmers, the testing group."

Whether or not problems are intentional, the first step enterprises should take when offshoring code development is due diligence, so that a relationship can start with a

offshoring code development is due diligence, so that a relationship can start with a reasonable degree of trust. "Start with someone you think will do the right thing, tell them what the right thing is, follow up, and then everyone is happy," says Richard Hunter, VP and research director at Gartner Executive Programs.

Part of that is considering the country in which the programming will happen. "It's an issue that worries the big vendors, companies like Microsoft, IBM and Sun, because they all have some of their development done in places like China, and China has written the most about how to attack the U.S.," says Bill Neugent, chief engineer for cybersecurity at MITRE.

Choosing a vendor becomes tricky, because there's also the growing trend of re-offshoring, or subcontracting outsourced contracts to other foreign service providers.

"Some Indian firms are sending managers to the large Chinese cities and outsourcing work there," says Marcella. "Unless I specifically state in the contract that the third-party provider can't re-outsource it, what's to keep them from outsourcing it to Beijing?"

Beyond checking references, specific due diligence on the offshore provider and all personnel who will have access to the code should be done by someone in the country who is familiar with its customs and laws. A company that can offer coverage in one area might be a poor choice in another. "We know China and Japan, for example, but couldn't help with New Zealand and Australia," says Richard Isaacs, senior VP at The LUBRINCO Group, an international risk management firm.

Contracts must obviously cover all the salient points, so each party knows its obligations and responsibilities, but not before corporate representatives examine an offshore company and its method of doing business. Recently, a client of the law firm Shaw Pittman sent a group to examine a number of offshore code development candidates. "They were distressed by what they saw operationally at one potential vendor," says Akiba Stern, a partner in the New York office. "I think they thought the security was more lax than they expected."

Even when a company seems competent and alert, direct involvement can't end. A contract must explicitly cover the approach to security and code quality, including specifications of penetration testing, the handling of security incidents, code testing, and an overlapping code review process so there are checks and balances on work. The client company should make use of Web conferencing to participate in design meetings and reviews.

James Kalyvas, chair of the e-business and information technology practice in the Los Angeles office of the law firm Foley & Lardner, also stresses the ability to withdraw from the agreement if things go wrong. "Having the right to get out and actually getting out are two different things," he says. The client needs copies of regular data backups, code, documentation, and any other item that would be necessary to bring a project in-house.

Such preventive activities may seem overkill, as no obvious security problems from offshore code development have hit the news. But the time may be coming, says consulting firm [SeigeWorks](#), which had a client outsourcing code work to India.

"Two years into the development, we did an assessment and found major vulnerabilities," says CEO Jeff Bennett. "These guys are paid to get the stuff [done] quickly, and security slows down the speed of the coding."

Precautions may seem excessive, especially when a company is looking offshore for cost savings. But experts say the upfront costs may negate the expensive code repair or, worse, security incident recovery.