



**DO YOU KNOW WHERE YOUR CODE IS WRITTEN?
AND BY WHOM?**

By: Jim Astrachan

Cyberterrorism? Sleeper bugs and back doors? Gangster programmers? The new trend of outsourcing software code development overseas may make these occurrences more likely than they were when companies wrote their software code in-house using programmers and supervisors who were well known employees..

According to industry research, outsourcing the software programming function to overseas venues is a growing trend, unlikely to slow at any time in the next decade. Although some say that President Bush's Economic Initiative will result in two million new domestic jobs, three million American programming jobs are likely to migrate to foreign shores in the next ten years. The reason for this, of course, is savings of almost forty percent of what the same code would cost if written in America by programmers earning upwards of \$75,000 per year. Forrester Research of Cambridge, Massachusetts estimates that 70 percent of these three million programming jobs will move to India, 20 percent to the Philippines and 10 percent to China. That's a loss of two million programming jobs to India alone. For the cost of one American programmer, a company can hire four or more Philippino programmers.

Some of this offshore software is providing crucial functions for American businesses and financial institutions, and security experts, including highly placed persons in our government, are concerned. They should be. Imagine how much damage could be inflicted on a bank or a brokerage house by a terrorist or gangster who infiltrates a Philippino technology services company. The prospective problems are three-fold. Money can be diverted to finance acts of terrorism, confusion could be created to materially and adversely affect our economy, and crooks can program code to steal money from the company cash register.

American businesses are not only directly hiring foreign companies to write their code, but American technology service companies, like EDS, are also opening foreign offices where code is written for their United States customers in order to profit from cheap labor. The customers of some American technology service companies have no clue that their code is written offshore.

Depending upon whom you talk with, the problem is either imaginary, or the chance of code-related treachery is imminent. It is no surprise that those technology service firms employing overseas facilities to write code for their U.S. customers claim there is no problem. Nor should anyone be surprised to learn that many of the warning cries come from the mouths of American programmers, both working and not working.. But, outsourcing of code writing has the government concerned and not just with overseas venues, as internal saboteurs and crooks have an opportunity to wreck havoc with the software projects on which many American businesses depend.

For any business intent upon taking advantage of what might appear to be lower programming costs, there are protective steps that can be taken and whatever belief a business has, its officers can be criticized if they do not attempt to add a layer of protection to the process. The critical first step is to assess the potential level of harm that could befall the company if the software was tampered with. In other words, is the software critical to operations? If it fails, will the business shut down? Might it allow a programmer, or his master, living 3,000 miles away access to the bank vault? If the answer to any of these questions is yes, it may be wise to insist that the code be written in the States. Sensitive code usually is, and there's a good reason for this. But even United States sourced code is not tamper-proof.

Regardless of whether the outsourced programming is done in Kansas or Madras, it is essential to know a lot about the people who own, and work for, the technology service company doing the programming. This process becomes something in the nature of a private security clearance, but this may be a hit or miss proposition unless the process of investigating and clearing all personnel involved with the code is standardized and the results carefully reviewed. And, in the typical field situation involving a large software project, many people contribute code and the turnover of personnel is constant. Making sure that only cleared people work on the project is a challenge, but this criteria must be carefully and thoughtfully addressed in the software development contract, as should a thorough understanding of where, geographically, the code will be written.

In addition to identifying and clearing all persons with access to the developing code on an ongoing basis, numerous reviews must be performed on the code by the

technology service firm's quality control department. Traditionally, however, these reviews are undertaken to determine only functionality, robustness and supportability of the code. In addition to these traditional reviews, the technology service firm must also be required, by contract, to review the software to determine whether sleeper bugs or back doors have been embedded deep within the code. This task is much more difficult and will add cost to the project. But this added cost is not nearly as high as the damage these bugs can cause to an unsuspecting business.

As a safety measure, the business whose software is programmed should employ a knowledgeable and independent third person to audit the security clearance procedures and reviews conducted by the contractor. Someone who is very familiar with the country. As an additional level of protection, the third party can conduct its own security clearance and code reviews. These steps add cost but may be well worth the price. This review must be ongoing until the project is complete. This cost should be built into the development budget. Finally, because it is well to remember that those intent on causing harm can easily do so from inside our borders, these rules apply to any outsourced code; made in America or not.

James B. Astrachan is a principal of Astrachan Gunst Thomas & Ahn, P.C., a Baltimore based intellectual property firm. Mr. Astrachan is a former and founding chair of the Intellectual Property Committee of the State Bar Association and can be reached at www.agtalawyers.com.