

Federal Computer Week

JULY 19, 2004 • VOLUME 18 NUMBER 24 • FCW.COM

Smart government starts here



Holes in outsourcing

As more software is developed overseas, concerns grow about the security of critical systems

PAGE 60

The outsourcing hole

As more software development is shifted overseas, concerns grow about security

BY MATTHEW FRENCH

It's a story that could come from a Tom Clancy book — a terrorist cell looking for an advantage against the powerful U.S. military trains a group to be software programmers, who then infiltrate companies that have sent their software development work overseas. Working for those companies, the programmers surreptitiously put vulnerabilities in software.

The concept may seem far-fetched, but so did using planes as weapons prior to Sept. 11, 2001. And given the importance of networks in the nation's day-to-day activities and in military operations, information security is even more critical now than it used to be.

As more technology work — specifically code writing — is outsourced to cheaper labor overseas, lawmakers and industry insiders are becoming increasingly concerned with what could amount to a large hole in the Defense Department's vaunted security.

For various reasons, DOD officials have made a concerted effort in recent years to purchase commercial off-the-shelf (COTS) software rather than develop it in-house.

The problem they face, however, is that the vendors on which the military has become dependent are sending much of their software development work overseas to cut costs. Offshoring may make economic sense for the companies, but the security ramifications are starting to

raise red flags for Congress, the Pentagon and some vendors.

At a meeting of the House Armed Services Committee last year, Eugene Spafford, a professor of computer sciences at Purdue University, said that anyone with an Internet connection can get the information necessary to launch a successful cyberattack on virtually any computer network.

“With bulletin boards and discussion lists... anyone can learn sophisticated attack methodologies,” he said. “There is a virtual worldwide training camp going on on a continual basis.”

In recent years, DOD officials have shifted their focus to buying proven commercial products. Unfortunately, holes repeatedly emerge in the code, which require patches, and the code is often written by people in foreign countries with no security clearance, some experts said.

“Over the past two decades, the policy of using COTS products whenever

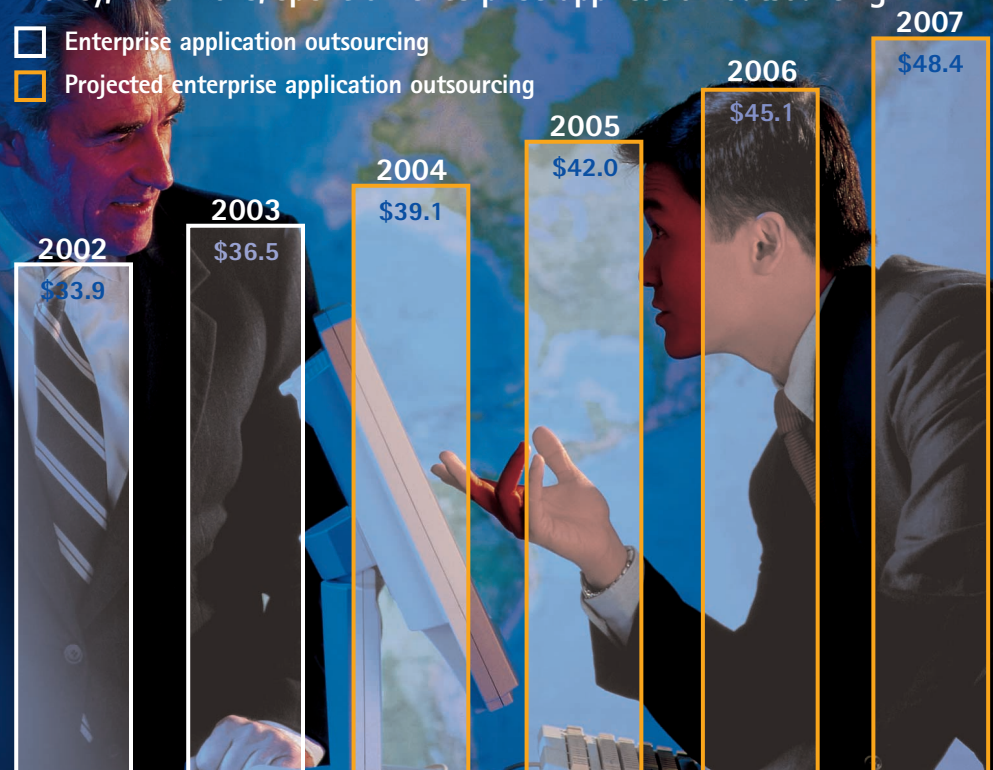
Over there

The practice of outsourcing software development may be fraught with potential security risks, but it is here to stay because companies save far too much money by having lower-paid Indian, Chinese and Russian developers write the code for their applications. Officials from market research firm Gartner Inc. predict that the money spent on enterprise application outsourcing will reach nearly \$50 billion by the end of 2007.

Source: Gartner Inc. report, “Forecast for Information Technology Outsourcing Segments Shows Strong Growth”

Money, in billions, spent on enterprise application outsourcing:

- Enterprise application outsourcing
- Projected enterprise application outsourcing



possible has provided a great benefit to the military and the taxpayers,” said Spafford, who also is director of the Center for Education and Research in Information Assurance and Security at Purdue.

“But there are some downsides to the department’s increased dependence on COTS,” he added.

Namely, much of the commercial software that DOD agencies use was never intended to be subjected to the significant threat level of the department’s networks. Spafford noted the inability to determine the code’s authors or their intentions or politics.

Using foreign labor “has been wonderful for the economy,” he said, “but it has introduced tremendous vulnerability to our software.”

Mounting evidence

The House version of the 2005 Defense Authorization bill contains a section that offers up to \$50 million in grants for DOD contractors to explore alternatives to outsourcing jobs. Among the strategies:

- Cutting costs.
- Programs to retrain workers.
- Technology development.
- Plant upgrades.

Yet a July 2003 Gartner Inc. report states that corporate spending for offshore information technology services will increase from \$1.8 billion in 2003 to \$26 billion in 2007, and work going to India will account for about half of that \$26 billion figure.

A June 2 Congressional Research Service report addresses outsourcing concerns and warns that they could be an issue that Congress must face in coming years.

“An increase in offshore outsourcing of high-tech jobs, including computer programming and chip manufacturing, may enable a transfer of knowledge and technology that may eventually threaten U.S. global technical superiority and undermine current [network-centric warfare] advantages,” the report states. “Contracting for national defense is reportedly among the most heavily outsourced of activities in the federal government.”

On the other hand, members of Con-

gress recognize the need for the federal government to rely on commercial software for both cost and security reasons. Commercial applications have long proven to be less expensive and less time-consuming than customized ones. The trade-off comes, according to some industry experts, at the intersection of cost savings and security.

“Observers have stated that companies that ignore outsourcing trends do so at the peril of their long-term competitiveness,”

A growing demand for software accountability

Concern among government and private-sector officials about secure software code will lead to new demands on the software industry, said Brian Kelly, director of the Giuliani Advanced Security Center. Among them will be demands on vendors for:

- Due diligence in providing assurances that software applications are trustworthy and secure.
- More care in developing requirements for software coding jobs that are sent overseas.
- Removal of sensitive portions of software coding such as business logic or security from jobs sent overseas.
- Testing of software much earlier in the development process.
- Software warranties or service-level agreements that hold vendors responsible.

— Matthew French

the report reads.

A Government Accountability Office report issued May 25 states that DOD officials’ control over software, particularly that which goes into weapons platforms, is lacking.

“DOD acquisition and software security policies do not fully address the risk of using foreign suppliers to develop weapon system software,” according to GAO’s report, titled “Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks.”

“The current acquisition guidance allows program officials discretion in managing for-

eign involvement in software development, without requiring them to identify and mitigate such risks,” the report continues.

“Moreover, other policies intended to mitigate information system vulnerabilities focus mostly on operational software security threats, such as external hacking and unauthorized access to information systems, but not on insider threats, such as the insertion of malicious code by software developers,” the report states.

A quick fix?

Executives at some companies have already recognized the business opportunities associated with plugging security holes and are working to capitalize in that narrow field, especially with government agencies.

Ounce Labs Inc. in Waltham, Mass., has developed a tool that scours lines of code for potential security flaws, holes or errors. In addition, the company’s officials, working closely with one of the nation’s largest law firms, have developed contractual language that, for the first time, places the onus for the security of software on the developer.

Software development companies have always had a certain degree of responsibility for whatever patches and fixes are needed to plug security holes, but the new contract language brings culpability to a new level, according to Jack Danahy, Ounce Labs’ chief executive officer.

“Companies are in a state of uncertainty right now because of the financial pressures to outsource the code-writing work,” Danahy said. “Basically, what we’ve done is written contractual language that tells a software developer that if the purchaser finds a problem in the codes, the developer will fix it on their own dime.”

Code review is typically a laborious and expensive process, often requiring experts to spend days poring over lines of code, looking for mistakes or flaws.

“We founded the company to identify where security vulnerabilities exist inside applications,” Danahy said. “Our tool doesn’t just look at the code itself, but looks at it in context. It looks at the code in a different way and can expose more potential security flaws.”

He said companies need to be held to a higher standard than they are now when it comes to providing software that keeps the federal government running.

Linux worries

Another potential hole comes with the introduction of open-source software, such as Linux. Linux writers and advocates attest to its security, but others say that software written and examined by the masses cannot be truly secure.

Dan O’Dowd, president and CEO of Green Hills Software Inc. in Santa Barbara, Calif., said Linux advocates argue that a “many eyes” approach to security is as good as any test DOD officials could create.

“It’s false security, pure and simple,” O’Dowd said. “The argument that nobody could possibly slip by subversive code simply because a lot of people get to examine the code makes no sense.”

He argued that many Linux programmers are not U.S. citizens, and someone with malicious intent could easily develop a Trojan horse, a back door into the application or a time bomb.

“We have to recognize who we’ve been up against so far,” O’Dowd said.

“It’s been script kiddies in high school and college and pranksters. The people we need

to worry about — and haven’t been — are the professionals,” he added.

What comes next?

Michael Rasmussen, an information security analyst with the Massachusetts-based firm Forrester Research Inc., said the key to code security is oversight from the beginning.

“What is needed is software assurance in the development of the contracts, whether the contracts come directly from DOD or from one of its business partners,” Rasmussen said. “Commercial software might have a back door, and DOD needs to work with vendors to put in contract language that gives a level of assurance through code audits and reviews.”

Rasmussen said government agencies also should demand certain warranties that would include appropriate damages levied

against offending vendors if they don’t follow through with security measures.

Brian Kelly, director of the Giuliani Advanced Security Center, a joint venture between former New York City Mayor Rudolph Giuliani’s consulting firm and Ernst & Young LLC, said the concerns government officials have are shared by their counterparts in the private sector. But, he added, outsourcing isn’t going to stop now.

“Economics are dictating software development, and as much as vendors aren’t really comfortable with it, the financials of outsourcing will continue to drive it,” Kelly said.

“For too long, customers have been willing to accept software in whatever condition they receive it,” Kelly said. Then, they take the time to fix and patch it. “But [public- and private-sector officials] have begun to say, ‘Enough.’ Vendors are going to be held accountable to meet a minimum in quality.” ■

FCW.COM DOWNLOAD

Find a link to GAO’s report on the FCW.com Download’s Data Call at www.fcw.com/download.

Setting boundaries

On Oct. 30, 2002, Defense Department officials issued the Interim Defense Acquisition Guidebook, which contained the following security rules for when foreign nationals participate in software development:

- Vendors must indicate whether foreign nationals participated in any way in software development, modification or remediation.
 - Foreign nationals employed by contractors or subcontractors to develop or modify software code for DOD must have security clearances equal to the level of the program in which the software is being used.
 - Primary vendors on DOD contracts may have subcontractors that employ cleared foreign nationals who work only in a certified or accredited environment.
 - DOD software with coding done in foreign environments or by foreign nationals must be reviewed by software quality assurance employees for malicious code.
 - Vendors that demonstrate efforts to minimize the security risks associated with foreign nationals will be given preference during the contracting process in product selection or evaluation.
 - Software quality assurance employees must check software sent to locations not directly controlled by DOD or its contractors for malicious code when it is returned to the DOD contractors’ facilities.
- This guidance acknowledges the additional risks associated with using foreign nationals in software development, but the procedures listed are not mandatory and, according to the guidebook, are to be used at the discretion of acquisition program managers.

— Matthew French

