Trading Security Away

Offshoring puts our information sector at risk, though the greater danger may come from lost expertise rather than a cyber-attack.

By W. James Antle III

THE USUAL homeland-security nightmare scenarios focus on hijacked airliners or suitcase nukes being shuttled into the country by terrorists. But in today's information-based economy, should we be just as concerned about the cubicles where our software code is written? As dependent on intricate computing and telecommunications systems as the United States has become over the last decade, the security of our information technology (IT) capabilities is impossible to ignore.

Ask people about the relationship between technology and national security, and the question immediately conjures Hollywood-style images of al-Qaeda cell members huddled in Internet cafes unleashing electronic Armageddon on major American cities. In an era of terrorism and rising anti-American sentiment throughout the world, such doomsday scenes cannot be dismissed entirely. But perhaps they overshadow the likelier threat to our safety from rising dependence on others for our country's technology needs.

The issue has gained new salience as companies increasingly move key IT functions and infrastructure to foreign countries, where they can operate at a lower cost than in the domestic market. Offshoring is usually discussed in the context of dollars and cents: the money companies save on the bottom line by farming out such tasks as software development to low-cost labor markets or the impact on the jobs and wages of American technical professionals. But some now question whether the practice exposes software source codes and IT infrastructure to heightened risk.

Concerns about computers being used as weapons are not new. In February 1998, as the U.S. was preparing for possible military operations in Iraq, the Solar Sunrise attacks were carried out against Defense Department computers worldwide. Hundreds of network passwords were obtained, and many key systems on unclassified networks were affected, although nothing mission-critical was compromised.

The attackers did not turn out to be terrorists or Iraqi saboteurs. Instead, they were two teenagers from California and one from Israel. Instead of being reassured, government officials wondered what more sophisticated attackers could have done. The incident helped the term "cyberterrorism" gain currency, with experts warning about the possibility of hackers logging on and shutting down power grids, opening city water valves, or disabling telephone networks, which became the subjects of articles, academic papers, and hearings. Congressman Lamar Smith (R-Texas) famously proclaimed, "A mouse can be just as dangerous as a bullet or bomb."

Businesses and government responded with heightened IT scrutiny. According to the Gartner Group, by 2001 companies were spending at least $3.6 billion annually on security software alone. But many industry insiders argued that major cyberattacks on the level often referred to as "Electronic Pearl Harbor" were unlikely because of the amount of time and resources they would entail. A 2002 study by the U.S. Naval War College concluded that an attack of that magnitude would require five years of planning and $200 million in funding. Viruses, often written by people no more technically advanced than the Solar Sunrise attackers, have become a frequent and costly nuisance but hardly anything likely to bring the economy to its knees.

Much of the preparation for Y2K—when businesses feared that their systems would confuse 2000 for 1900 and checked software line by line in an effort to avert service interruptions—was done by foreign programmers. When incidents of resultant sabotage and theft proved to be as rare as major Y2K-related outages, many companies came to the conclusion that apprehension about moving programming work offshore was unwarranted.

CONGRESSMAN LAMAR SMITH (R-TEXAS) FAMOUSLY PROCLAIMED, "**A MOUSE** CAN BE **JUST AS DANGEROUS** AS A **BULLET** OR **BOMB**."

LICENSED TO UNZ.ORG
ELECTRONIC REPRODUCTION PROHIBITED

Today much more of American businesses' IT operations are offshore, in countries ranging from India to China, with the world political climate much different—and more dangerous for Americans—than on New Year's Eve 1999. Industry watchers claim that the opportunity and incentives for mischief have increased, and no Electronic Pearl Harbor-like resources are necessary to take advantage of them. Programmers will have ample opportunity to write "Trojan horses" into software or simply steal information, whether acting on behalf of terrorist networks, organized crime, or foreign intelligence agencies—or simply for their own personal reasons.

So far no major breach has been discovered, though examples of smaller ones are legion. David Lazarus of the *San Francisco Chronicle* reported that a Pakistani clerical worker warned UCSF Medical Center in California that she would post patients' confidential records on the Internet unless she was paid money she claimed to be owed. The woman ended up receiving about $500 from someone Lazarus described as "another person indirectly caught up in the extortion attempt" and withdrew her threat to post the medical files online.

It's the kind of problem that suggests more to come. David McCurdy, a former congressman who now serves as the executive director of the Internet Security Alliance, told the *New York Times* that the risks inherent in offshoring are "the most serious of the industry-based issues that this country faces."

Merry Christmas

The American Conservative **will publish its next issue in four weeks instead of the usual two. Our editorial offices will reopen Jan. 3.**

But the UCSF incident could just as easily have been perpetrated by an American with similar motives. A recent Heritage Foundation study suggests that the threat is exaggerated. Senior homeland security research fellow James Jay Carafano and senior legal research fellow Paul Rosenzweig found that IT work can safely be moved to countries that respect "the rule of law, transparency, and open competition."

PROGRAMMERS HAVE AMPLE OPPORTUNITY TO WRITE "**TROJAN HORSES**" INTO SOFTWARE OR SIMPLY **STEAL INFORMATION**, WHETHER ACTING ON BEHALF OF **TERRORIST NETWORKS**, ORGANIZED CRIME, OR **FOREIGN INTELLIGENCE AGENCIES**.

"Are there risks involved in outsourcing? Absolutely," Carafano acknowledges. "But those risks are the same whether you outsource to India or Illinois." He argues that the onus should be on companies to ensure that they contract with firms that have effective security controls. "It comes down to two words," says Carafano. "Due diligence."

The Heritage study points to efforts by the National Association of Software and Service Companies (NASSCOM), India's leading IT industry group, to bring Indian regulations into line with U.S. industry standards. "We're not talking about lowering the bar at all," Carafano says. "We're not advocating complacency. But countries are learning that if they want to participate in the global economy, they have to meet certain standards."

According to the Forrester Research Group, some 70 percent of the IT jobs headed abroad by 2015 are en route to India. But some 20 percent are headed to the Philippines, a country wracked by terrorism, and another 10 percent to China, a country many view as a potential competitor to the United States. Doesn't this make a difference?

Carafano says that the overall legal and political climates are more important in an offshoring destination are more important than the prevailing ideology. "Then you have to evaluate it at the individual provider level," he says.

Standards vary not only among countries and offshoring service providers. Companies that outsource also differ in their approaches to protecting offshored tech assets. The Meta Group, a leading IT consulting firm, found in a study of the European industry that only 58 percent of companies that outsource security services work with their outsourcers to ensure that effective controls are in place. Only 57 percent review the security procedures the firms they outsource to put in place. And as many as 44 percent fail to keep primary responsibility for establishing security procedures within their own company.

"Wherever you outsource you need to have a good service level agreement," says Paul Proctor, Meta's vice president for security and risk strategies. "You need to ask, 'What are the threats to those assets while they are offshore?'"

Carafano believes that the government could play a constructive role in disseminating information. "Markets work when there is transparency," he says. "What would the shareholders of those companies say if they knew that they weren't following all of the industry's standards?"

Ron Hira, assistant professor of public policy at the Rochester Institute of Technology, argues that the national-security risks of offshoring are real but more complicated than the isolated acts

LICENSED TO UNZ.ORG
ELECTRONIC REPRODUCTION PROHIBITED

of rogue software engineers. "I think that businesses will ultimately figure out how best to secure their own infrastructures," he says. "That's not the only homeland security problem, even if it is the most obvious one."

According to Hira, the pressing problem is the loss of America's ability to maintain its technological edge over the rest of the world. "Technological superiority is the key to our military superiority," he says. "It's not an accident that so much of our technological innovation has been driven by defense procurement."

As IT work moves offshore, two things happen. One is that the field becomes less attractive to domestic workers, so Americans have less incentive to pursue high-level technical knowledge. While the overall economic impact of offshoring is still being debated, there is growing evidence that it is deterring people from the field. Enrollments for advanced degree programs in engineering and computer science have declined significantly.

The second problem is that when technology is concentrated in inexpensive overseas labor markets, the U.S. military has less ability to influence innovation and encourage the development of needed products through procurement. And the U.S. government necessarily comprises a smaller share of the world market than the domestic market, further diluting its potential impact. Market incentives may exist for companies to protect their data, but not the military's technology edge. "We're not just offshoring infrastructure, we're offshoring creativity and innovation," says Hira. "When the military has technology development needs, they're not looking for the cheapest. They are looking for the best. Will they still be listened to as much if they are a small customer?"

A Congressional Research Service report release in June echoes these concerns: "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 advantages."

Hira points out that national-security needs have long driven major U.S. technical advances. The Soviets' launch of Sputnik in 1957 spurred science-education initiatives across the country. NASA bought the integrated circuit from Texas Instruments in 1959. IBM's early computing research was heavily funded by government procurement. Microsoft was originally based not in Seattle but Albuquerque, near the Department of Energy. "Nearly every breakthrough in automation and electronics has had some link to government," says Hira.

Just as the economic debate over the movement of the technology sector overseas has mirrored earlier exchanges over the export of manufacturing jobs, so does the debate over its national-security dimensions. Even if the United States can survive economically without a manufacturing base, is its national-defense posture compromised by a reliance on foreign producers? Given the centrality of technological advantage to America's status as a military superpower, the question may be even more important when discussing the manufacture of computer chips than steel.

The answer may be found in an honest look at the long-term ramifications of offshoring—and an acknowledgement that it may yield costs as well as benefits. ■

Mausoleum of Modern Art

The new MoMA has the soul of a corporate HQ

By Robert Locke

NEW YORK'S FAMED Museum of Modern Art has just reopened after a three-year hiatus in which it nearly doubled in size. The architect of the new structure is the Japanese Yoshio Taniguchi, chosen over a field of prominent Western modernists and postmodernists. For while Japan has never been a hotbed of modern art, and the collection contains few Japanese works, it was a font of architectural minimalism centuries before Mies van der Rohe and Le Corbusier.

It seems that history has been no kinder to the ponderous philosophical claims of artistic modernism than to any other of the 20th century's great ideologies, and all we are left with is minimalism. And not even Western minimalism—as in the theoretically bristling, pseudo-mathematical constructions of Peter Eisenman or the cocaine-slick, *nouveau riche* flashiness of Richard Meier—but a contemporary version of a tradition that was mature when colonial Williamsburg was new.

Minimalism is a perfectly valid artistic style with a history that goes back fur-

LICENSED TO UNZ.ORG
ELECTRONIC REPRODUCTION PROHIBITED