

Common Sense

Offshoring Information Technology and National Security

A Connect-the-Dots Overview

Transferring Information Technology (IT) jobs and work to historically hostile (or “unaligned”) low-wage nations poses serious national security issues.

Known as “offshoring,” the number of IT jobs moved to low-wage nations has enormously increased since the dot.com bust in 2001. An estimated 400,000 IT jobs have already been moved to countries such as India, China, Jamaica, and Russia, and predictions are that in the next decade the number of jobs transferred will be in the millions.

In 1998, long before IT offshoring became widespread, FBI Director Louis Freeh warned the Senate Committee on Intelligence:

“Terrorists, transnational criminals, and intelligence services are quickly becoming aware of and exploiting the power of information tools and weapons. ... Perhaps the most imminent threats today come from insiders. Insiders have the advantage of not needing to break into computer systems from the outside, but only to use, or abuse, their legitimate access.”

From a national security perspective, three immediate threats stand out:

1. **Offshore research & development (R&D)** of vital corporate and government information processes, systems, and networks. This inevitably results in extensive dissemination of insider knowledge about operations and security protocols. Knowledge that could be used to misuse, capture, sabotage, or destroy those systems.
2. **Offshore administration** of government and corporate information systems and networks. This too means access to and penetration of those systems. The “outsiders” become the “insiders.”
3. **Offshore data-processing** of sensitive financial and medical information. The end result is the circumvention and collapse of privacy safeguards leading to serious threats of both corporate and individual blackmail. It will also result in illicit commercial exploitation of personal information.

THE OFFSHORE IT ENVIRONMENT

From a security standpoint, the following general characteristics of low-wage IT nations are key:

- **Inadequate Legal Framework.** Low-wage IT nations have either abysmally weak privacy & data-protection laws, — or they have none at all. And what regulations they do have are rarely enforced, while any violator so incompetent as to be caught is treated leniently.
- **Low-wages & poverty.** Corporations are offshoring their IT work because labor costs are dramatically less. A rough rule of thumb is that IT workers in low-wage nations are paid just 1/6th of what comparable positions are paid in industrialized nations. But no one, not Indians, Chinese, Russians, Jamaicans or anyone else enjoys poverty. When you combine a lax regulatory environment with very low incomes you have a work force that is highly susceptible to bribery, peculation, and freebooting.

- **Culture of corruption.** The low-wage nations to which IT work is being sent share a pervasive culture of corruption. The Center for Corruption Research in Europe annually scores nations on a corruption scale of 0 (most corrupt) to 10 (least corrupt), and then ranks nations in order from least to most corrupt. Their 2003 rankings make it clear that the low-wage IT nations are some of the most corrupt on Earth:

Country	Score	Rank
Canada & UK	8.7	#11
USA	7.5	#18
Israel	7.0	#21
Jamaica	3.8	#57
China	3.4	#66
India	2.8	#83
Russia	2.7	#86

[For the curious, the 3 least corrupt countries were Finland (9.7), Iceland 9.6), and Denmark (9.5). The 3 most corrupt were Haiti (1.5), Nigeria (1.4) and Bangladesh (1.3).]

This pervasive culture of corruption is well known and openly acknowledged by those countries that have a free press. For example, on May 17, 2003 *The Times of India* wrote:

“It cannot be denied that corruption is ubiquitous in our national life. In India, honesty and survival in elective office are increasingly incompatible. Centralized bureaucracy, life-time job security, and virtual immunity from punishment make public servants callous and corrupt. Inefficient and inaccessible justice, and absence of instruments of accountability make punishment for corruption difficult.”

In environments characterized by inadequate legal systems, low-wages, and high-corruption the promises by IT corporations that their offshore subsidiaries adhere to the same business and security practices as in the home nation are nothing more than PR twaddle. And the claims that offshore R&D and data processing contractors are held to some mythical “gold standard” of data security and privacy are even more absurd.

One of the few things that both the CIA and FBI agree on is that the two most common motivations for people becoming spies or turning traitor are blackmail and money. To begin looking at the money side, make the following hypothetical cost-benefit comparison:

- You are an IT professional in Silicon Valley earning \$120,000 a year. An intelligence service (foreign or domestic) or a criminal organization offers you a \$20,000 bribe to compromise your employer’s security. But that is only two-months pay versus a high risk of getting caught and punished severely. Moreover, merely being accused would result in your being barred forever from all future IT employment, to say nothing of the social ostracism you would experience in a culture that abhors such behavior. Hardly an attractive proposition.
- On the other hand, suppose you are an IT professional in Bangalore earning \$20,000 a year. An intelligence service (foreign or domestic) or a criminal organization offers you a \$20,000 bribe to compromise your employer’s data security. That’s an entire year’s pay. Balanced against that tax free money is a low risk of getting caught and an even lower risk of any significant punishment. And in your culture you would experience much less social ostracism. Very tempting.

POTENTIAL THREAT SOURCES

In his Senate testimony FBI Director Freeh reported:

“However, as commercial information technologies create advantages, their increasingly indispensable nature transforms them into high-value targets. ... These vulnerabilities are accompanied by a more variegated threat picture. The range of potential adversaries that may seek to attack U.S. infrastructure systems is broad and growing. Disgruntled employees, disaffected individuals or groups, organized crime, domestic and international terrorists, and adversary nations are all potential sources of attack.”

All low-wage IT nations have their own well-funded intelligence agencies (and in many cases they have multiple competing agencies). Can there be any doubt that the extensive Chinese, Indian, and Russian spy services have already inserted or recruited agents into offshore R&D contractors who are busy designing the global information systems and networks of tomorrow?

Can there be any doubt that they have also penetrated the data-processing centers being set up to handle the confidential medical and financial data of the Western world? And given the low wages of offshore IT workers, can there be any doubt that the secret services of other governments (to say nothing of terrorist and criminal organizations) will have no difficulty hiring their own insider agents?

INFRASTRUCTURE VULNERABILITY

Obviously, the most catastrophic threat we face is sabotage of critical infrastructure, — the electric power grid, the banking or air traffic networks, the internet backbone, and so on.

In recent years we’ve all experienced the disruption and cost of relatively trivial email viruses such as Melissa, Bugbear, SoBig, Klez, and so forth. Those attacks were mostly pranks perpetrated by hackers, — usually teenagers, — operating as outsiders. Imagine the damage that could be done by an insider, or a group of insiders, directed by a foreign intelligence service or terrorist organization.

Ponder just one of many recent news reports (*San Francisco Chronicle*, 11/5/03):

“Pacific Gas and Electric Company has been quietly out-sourcing critical design work [on] California’s aging power grid and some of the work is heading as far off as Thailand. This, say security experts and insiders at the utility, is a reason for Californians to worry. ... If that [information] got into the wrong hands, it could be used to sabotage the systems. ... Most of the out sourced information is unavailable to the general public...”

Sabotage and disruption are not the only threat. When spy agencies, drug cartels, and terrorist groups gain insider knowledge of the world’s financial networks they will use those networks to launder money, finance operations, distort currency markets, and so forth.

Moreover, a credible threat of infrastructure attack is enough to blackmail a government or a major corporation. “Unless you immediately do X, or stop doing Y, or pay us Z we will crash or compromise the _____ (fill in blank) network or system.” When you receive a message like that it is already too late because whatever choice you make — surrender or refuse — will result in disaster. In the 20th Century we feared nuclear blackmail, in the 21st we will face Information Technology blackmail.

Those who reap short-term profits from IT offshoring assure us that such fears are groundless because the sensitive secrets are “securely protected.” Nonsense. It is simply impossible to prevent those who design and administer critical information system from learning everything they need to know to misuse, manipulate, or crash those systems.

To give a benign example, a few years ago I worked for a major internet company whose name you would instantly recognize. Late one night after hours a problem occurred with a critical server. To fix it, we needed the Super User Root password, the password that grants all power over everything. This is the password that the system gods use, and only a select few were allowed to know it. Unfortunately, none of them were on duty or answering their pagers. But based on my general knowledge of how things were done at that facility it took me less than five minutes to guess what the password was. I used no programming skills or hacker technology, I didn't open any files I wasn't supposed to, I didn't sneak a peak at anything, I simply guessed based on my general knowledge of the company's operations and culture. Now imagine what an insider working for a criminal gang, terrorist group, or intelligence service would be able to learn over months and years of deliberate, directed, espionage.

LONG-TERM STRATEGIC THREAT

A century ago “national security” meant the military, — military threats, military defenses, military secrets. But in a modern industrial society the definition of “national security” is much broader. Today, the economy and the infrastructure on which it rests is as vital an aspect of national security as are the armed services, intelligence agencies, and weapons research.

The Federal government annually spends tens of billions of dollars to subsidize and support American farms and farmers. But why should urban taxpayers support farmers? Because the ability of a nation to feed itself is a national security issue. U.S. farmers cannot economically compete on the world market against low-cost or highly-subsidized farms in other countries. Were it not for the US subsidies, many American farms and farmers would go out of business and we as a nation would be increasingly dependent on foreign sources for our daily bread. In a time of crises a nation that cannot feed itself cannot defend itself, and we would be vulnerable to anyone who was able to threaten our food supply.

In the 1800s Britain dominated the planet both militarily and economically in large part because they were the world leaders in the critical technologies of steel, steam, chemistry, and mechanics. There is common agreement that in the coming century IT will be one of the absolutely critical sectors of the economy. Communications, defense, the economy itself will depend on information technology.

The U.S. military is pre-eminent today not because of its size, — several countries have more men under arms, — but because of its sophisticated technology and highly trained personnel. Developing, supporting, and underlaying that military technology and personnel-base is the American IT industry.

Our population of skilled IT workers are a valuable, — a critical, — national asset. We have a creative, highly trained, highly-motivated, workforce. It is in the national interest to nurture and enlarge that workforce for the future. But now IT jobs are being off-shored to low-wage countries and those of us currently in IT are being forced to find other occupations. Talk to the bartender at any Silicon Valley watering hole and odds are you're talking to a former engineer, programmer, or systems analyst. Nor will new people be entering the field. Why study computer science if all the cutting-edge jobs are in India, China, and Russia, with pay scales that an American teacher or auto-mechanic would scoff at?

If research and development are done elsewhere, the strategic reservoirs of skilled people will be elsewhere and so will the knowledge-base of technology and technique. It may be short-term profitable for the large corporations to off-shore their IT work, but it is devastating to our long-term national

economic and security interests. And a nation that is converting engineers with advanced degrees to taxi-drivers is headed for a serious reckoning.

PERSONAL DATA THREAT SCENARIOS

The data-processing of confidential medical and financial information is being offshored to workers whose sole reason for being hired is that they are paid low wages. And these workers live in cultures where making a little extra on the side is the norm. Moreover, the competition among off-shore data-processing firms is fierce and cut-throat. From time to time those companies are going to desperately need a little cash infusion to keep afloat. In such cases, selling information under the table to those who have some creative use for it is just smart business, — or simple survival.

For example, imagine that....

- You're a law enforcement agent working in drug enforcement. You believe in your work and you're extremely effective, you have the highest conviction rate in your jurisdiction. Unfortunately, a decade ago you were in rehab for addiction to pain pills. Though you've been clean and sober for ten years, under your department's "zero tolerance" policy you would certainly be fired if it came to light. A Jamaican contractor now does your HMO's data processing. One day a Colombian gentleman from Cali contacts you with a take-it-or-leave-it business proposition.
- You are an elected official in a tight re-election race. Several years ago you invested some money in a land deal that went sour. You did nothing wrong, but if your opponent got hold of the information he could twist it to appear as if you used your office for personal gain. Your bank has offshored your financial data to Guangzhou. Suddenly you get an email from China from someone you never heard of urging you to vote Yes (or No) on this (or that). Copies of your personal financial records are attached.
- You are a top executive of a transnational corporation and you are up for that final big promotion to the corner suite of the office penthouse. Unfortunately, a big item in your personal portfolio is a bloc of stock in your firm's main competitor. You hope the Selection Committee does not know about this. Your investment broker uses a data-processing contractor in Hyderabad. A week before they decide a man of indeterminate national origin and extensive foreign connections approaches you with some interesting new uses for your company's shipping containers. You know, those containers that are so familiar to Customs and Coast Guard that they almost never inspect them.
- You're a network manager for a key component of the East-coast electric grid. You live in a conservative suburban community with your wife and teenage daughter. You're active in your church and a member of the country club. You have also been diagnosed with HIV or some other sexually transmitted disease and your health records are now stored on a computer in Bangalore. If your condition became public knowledge you and your family would be shunned and humiliated. What little favor might you be willing to do for someone to prevent that from occurring?
- You're a tycoon of industry working on the biggest deal of your career. Unfortunately your holding company is experiencing some temporary cash flow problems that your potential new investors shouldn't find out about. Your corporation uses one of the Big-6 accounting firms because they are so accommodating to the needs of their mega-clients. But to cut costs their IT operations have been offshored to Novosibirsk. One afternoon a large, heavyset man with a thick Russian accent overlaid by Brighton Beach patois calls on you with a list of people he would like you to hire into key positions in your various subsidiaries around the world.

- You're a high-ranking Air Force officer in charge of an important weapon R&D program which requires that you maintain your flight status. Unfortunately you've developed a small, quite minor heart murmur which you've chosen to have treated by a private physician rather than the base Medical Officer. Now this information is in the hands of Chinese Military Intelligence. All they want (at first) are the public documents related to the project. Well, it's public information, why not? But now they have you on tape giving them military information, and now they want more.
- You're applying for [a new job, health or life insurance, a major business loan, etc.] You are shocked when you are inexplicably turned down. What you don't know is that a million medical records, — including your DNA scan that reveals you are at high risk for _____ (fill in blank), — have been sold under the table by a Bombay data processing contractor to a Hong Kong consulting firm. For an annual fee, insurance companies, banks, and corporate human resources departments can subscribe to the Hong Kong service and thus use your medical records as part of their confidential background checks and screening. The actual screening itself is done by their [Bangladeshi, Nigerian, Ukrainian] subsidiaries and is thus completely outside the jurisdiction of U.S. law.
- You're an upstanding, hard-working citizen with no arrest record and AAA credit. Unknown to you, one of the Big 3 credit reporting agencies has offshored its data work to Moscow. (No, not Moscow Idaho, Moscow Russia). Everything the KGB (or the Russian mafia) needs to steal your identity and use it to plant moles and operatives in U.S. jobs is stored on computers located a kilometer from the Kremlin. One day you are shocked when the FBI breaks down your door with an arrest warrant charging you with espionage or drug smuggling. "But, I'm innocent," you tell them. "You've got the wrong guy!" No need to worry though, if you have a competent hard-working attorney it will only take a month or two to sort it out.

— Sojourner, November 2003

[About the author: The author is an IT professional who has been employed by marquee-name hardware and software companies since 1980. "Sojourner" is a pseudonym because the author still has a job and wishes to keep it. In an environment where the White House outs an undercover CIA agent because her husband reported an inconvenient truth, the author is not optimistic about the reaction of a private IT corporation to a presumptuous employee daring to contradict the PR happy-talk.]