

The Canaudit Perspective

Volume 4, Issue 9
September 2003

Topics of Interest:

- Overseas Outsourcing of the Helpdesk Weakens Security
- System Development and Program Coding are Part of Critical Infrastructure
- Outsourcing Facilitates Cyber-Terrorism
- Data Ownership, Identity Theft, and Commercial Espionage
- We Must Fight Outsourcing to Preserve our Future
- Free Registrations for the IT Audit & Security Boot Camp

IT Outsourcing: Placing our Nation at Risk

By: Gordon Smith
President, CEO
Canaudit, Inc.

As many of my clients know, I like to write controversial articles for the Canaudit Perspective. This issue is no exception and very well may be the most controversial article I have written. Last week I was reading the September 29, 2003 issue of *Forbes Magazine*, when an article by Robyn Meredith immediately caught my eye. The title was certainly unusual – “Giant Sucking Sound” http://www.forbes.com/free_forbes/2003/0929/058.html – not your normal Forbes title. As I read it, I quickly understood that there were major ramifications for auditors and security officers that were not covered in the article.

The article, which describes the continuing outsourcing efforts at EDS, mentions that 4,000 white-collar jobs (i.e. engineering, programming, and accounting) are being outsourced overseas each week. These are not low-skilled manual labor jobs. Rather, they are jobs that, in my mind, should not be outsourced overseas. Yes, I understand the economic issues. Andy in Mumbai (mentioned in the Forbes article) earns \$1.25 per hour, is highly educated, and is certainly qualified to perform his helpdesk function. Certainly, the savings to the U.S. parent company are significant and make the company more competitive. While I am a strong believer in the free market economy, I also believe that outsourcing critical infrastructure jobs transcends economics and creates a clear and present danger to our country and our quality of life.

Overseas Outsourcing of the Helpdesk Weakens Security

Simple password resets may seem to be a trivial function to senior executives when they make the overseas outsourcing decision. In my mind, the ability to reset a password is very significant. By resetting the Administrator, DBA, or Superuser password on a system, the support person has the ability to take complete control of the server. If they have the ability to reset application passwords, such as PeopleSoft or SAP user accounts, then they may be able to gain DBA rights to the application or the database. Resetting normal user

passwords may give the support person the ability to commit fraud. They could add fictitious employees to the payroll, change the automatic deposit information for employee and vendor electronic payments, change customer addresses to redirect mail, or divert shipments of expensive commodities.

The overseas staff may also have the ability to copy files and databases or perform data extracts. This will enable them to glean an organization's data, which could then be sold to a competitor. Customer data, once copied, could be used to feed an international identify theft ring. It could also be used to commit loan or bank fraud, obtain California drivers licenses (as if it is not easy enough already), or even apply for and be granted a U.S. Passport using the pilfered identity of a U.S. citizen.

I have been an auditor now for over a quarter of a century. One thing that I have learned is that when new business concepts and technologies are originally implemented, the incidence of fraud goes up for a short period of time until new controls are implemented. In the case of help desk outsourcing, I am concerned that just one fraud against a broad customer base of an organization, such as a large American bank, could result in massive electronic theft. After the cost of the fraud and the negative publicity resulting from the defalcation, will the company that outsourced overseas still have an economic gain from outsourcing?

System Development and Program Coding are Part of Critical Infrastructure

Here in the United States we have some of the finest military equipment in the world. We have the best fighter jets, aircraft carriers, submarines, missiles, and advanced weapons known to man. I am sure that the Advanced Tactical Fighter or the new aircraft carrier USS Reagan could have been built much cheaper overseas. In spite of the higher costs, these critical assets were built right here in the United States. Why? We want to ensure that the technology remains ours! We want to ensure that these weapons are built in a secure environment and that they are not sabotaged. The same holds true for the strategic petroleum reserves. These reserves are not located overseas. Our strategic petroleum reserves are stored right here in the continental United States. I am sure it would be cheaper to pay the overseas suppliers to store and deliver it to us "just in time," as we do with manufacturing components. However, it is just not prudent to do so.

Corporate America is rushing to outsource the development of new systems and maintenance of existing systems to countries with lower wages. Imagine the damage and destruction that would occur if customer bank account data, factory orders, or other mission critical databases were downloaded then erased using an administrator account. How large of a ransom would a large bank pay to successfully recover a stolen customer account database. How much would a credit card company pay to recover customer credit card balances that mysteriously were erased from the storage area network and all backups? All it takes to pull this off is some sleeper code placed into an application that can be activated at will. Since neither new code nor changes to code are reviewed line by line on a regular basis, it would be possible to insert the sleeper code into the programs and wait for the right moment. While this may seem to be an unlikely scenario, unless there are strong controls over outsourced programming resources then a data hostage situation could occur.

Outsourcing Facilitates Cyber-Terrorism

Now that we have covered fraud, let's take the scenario a step further. On September 11, 2001 we learned just how dangerous a few box-cutters could be. Now imagine the damage that could be done if a coordinated attack was made on Corporate America through sleeper code as mentioned above, time bombs, embedded viruses or worms, or other new techniques. The targets could be SCADA systems that control our electric and gas utilities, emergency 911 systems throughout the country, the New York Stock Exchange, airline reservation systems, order entry and shipping systems, hospital and medical applications, and the top 200 banks. Maybe a cyber-attack would shut down air traffic control systems or water purification plants. While this might be a good plot for a futuristic science fiction novel, I believe that with proper planning and coordination, overseas programmers could insert the required code into programs or database applications **AND THAT THE CODE COULD GO UNDETECTED.**

Many of the controls that were in place in bygone days, such as source code review, have disappeared. In many organizations, program change control is weak or nonexistent. I had a client who mentioned that the integrators had complete control over the project. They write the specifications based on client input; they engineer the solutions; and they code, test, and implement the software. At the end of the project, the integrator will turn the software over to the client upon acceptance testing. This is a fairly common occurrence. Our clients use integrators, because they do not have the skills nor do they want to hire and retain the skills to implement ERP systems. Some of the integrators outsource their coding overseas and this could lead to our downfall. (As an example of what can go wrong, review the case of Hershey: http://www.cio.com/archive/111502/tl_hershey.html and <http://www.philly.com/mld/philly/business/4416908.htm>.)

In my opinion, the likelihood that a cyber-terrorist organization could do significant damage increases as the software industry consolidates. There are fewer vendors, and more code is farmed out to overseas entities. Also, as in-house programming decreases, reliance on software vendors increases. Outsourcing product development is old hat for the larger software firms. They have outsourced this work for years. As more organizations standardize on these purchased software solutions, the risk of cyber-terrorism increases.

Data Ownership, Identity Theft, and Commercial Espionage

More data is being sent overseas or is accessed by employees who are not in North America. Some banks have moved part of their customer service operations overseas. Other banks are experimenting with expatriating our data. Your name, address, social security number, and bank balance can be viewed by individuals overseas. Many manufacturers have sourced their manufacturing operations in other countries to save on labor costs and the ever-increasing costs of complying with government and social obligations. The ability to build their products is in the hands of foreign entities. Now we are sourcing our information systems and customer management overseas! The outsourcers are talking directly to our customers through the miracles of modern Voice Over IP (VOIP) networks, documenting quality issues with our products, and learning how to effectively market to the North American consumer. High-tech companies which make some of the products we need for transportation, communication, computations, and many

other products required to support our daily lives are outsourcing design, engineering, and even product testing overseas.

Let us look at what this means if we are an American technology company. We outsource design and engineering to Taiwan and Singapore, manufacturing to China, systems development to Pakistan, and information processing and customer service to India. Next we farm out backroom operations, such as accounting and procurement, to India or Eastern Europe. As companies outsource the majority of their operations overseas, it is only a matter of time until someone starts to silently and secretly acquire “control” of the Chinese manufacturing, the Indian information operations, and the engineering and research centers through a complex web of shell companies. In some cases, it may be through the purchase of these operations from the American parent; in other cases, they may acquire the intellectual capital of these firms.

By hiring the target company’s overseas employees, they gain the knowledge required to compete against the American firm. By bribing existing staff members or hiring “consultants” to acquire new product designs before they are patented, this new business operation could outmaneuver the American company and capture market preeminence. The overseas combinations could pilfer existing product technology that can be “reengineered” to create a competing product. This would decimate sales and eventually the profits of those companies that are outsourcing critical infrastructure to overseas operations. If this scenario becomes a reality, what will we have left in America? – High paid executive positions, low paid service industry jobs, and white-collar workers on unemployment insurance and welfare!

I recently discovered that the Final Four accounting firms are outsourcing or considering outsourcing the completion of tax returns overseas. Tax returns in the United States are considered confidential. The IRS strives to ensure our privacy. Now that this information is being exported, you can bet that at some point some of this confidential data will be disclosed. This confidential tax information could easily be used to commit fraud, identity theft, or to enable a terrorist to get a real U.S. passport using the name of a real U.S. citizen.

The Gradual Side

Last week I was in Pittsburgh teaching a class. I have to say that I love work assignments in this city. The people are highly educated, polite, and helpful. When I started my career in audit and security, this city was one of the leading business cities in America. It was the center of the steel industry. Banks and financial institutions filled the downtown core. Over the years, the steel industry was decimated by cheap, high-quality imports. The banks and financial institutions merged and then were acquired. Over time, jobs left the city. Some people moved to new jobs in other cities, eroding the tax base. Now, the city is in financial difficulty.

There was one highly skilled IT auditor in my class who lost his job to outsourcing two years ago. Just recently, he found another IT audit position. I have another client in the Allentown area. He worked for a company that was acquired, and then the audit department was outsourced. He has been out of work for over a year despite his strong proven technical audit skills. Why does it take so long to land a job? There are no jobs to

be had. If a job is available, it is taken by the lowest bidder! Last night in Minneapolis, where I am performing a penetration audit, I met with a security officer who I have known for over ten years. He is a topnotch professional who is recognized nationally for his capabilities. He is now unemployed, as his company decimated two layers of management. How long can we continue to lose jobs?

Bucking the Trend

I was in Tulsa in early September. This city was once a major growth area in the heart of America. Many of the banks were swallowed and jobs disappeared. High-tech manufacturing and maintenance, a cornerstone of the Tulsa economy, declined as jobs were sourced elsewhere. Even the oil industry, which for years drove the prosperity in this region, has consolidated. As each of these industries sank into economic duress, the citizens of Tulsa tried to cope with change. Finally, they hit upon the right idea – *Vision 2025*. This was a proposition that was put to the voters – to raise sales taxes to fund job and community growth. The additional taxes will be used over the next 22 years to encourage industry and to keep jobs in America (<http://www.tulsaworld.com/Vision2025Articles.asp>). The city will fund incentives to companies to build and grow in Tulsa. The city will fund the arts and may support the economic regeneration of the famed Route 66 to invigorate tourism. It has only been a month since this measure was passed by the voters. Already, several companies announced they will be expanding their operations in Tulsa. They and companies like them will bring jobs back to this lovely community. The people voted, they want to work, and they are willing to tax themselves to pay for the improvements needed to bring the jobs to their community. My hat goes off to the citizens of this city and the politicians who made *Vision 2025* a reality.

We Must Fight Outsourcing to Preserve our Future

If Tulsa can do it, so can the rest of America! Henry Ford implemented the 40-hour week as both an efficiency measure and a marketing ploy. By increasing leisure time, he built demand for his product – the automobile. In today's economy, the outsourcing trend is continuing, and the ranks of the unemployed and those who are living below the poverty line are growing. As a result, demand for products will decrease. Could this be the real reason behind the faltering economy?

If the middle class is outsourced, who is left to buy products? What future do our children and grandchildren have? We must buck the trend. We must fight for jobs, one at a time. Behind each lost job is a lost hope or dream. Behind each lost job is a family that will suffer hardship. Behind each lost job is the economic impact of a reduced tax base. This puts economic pressure on the city, state and national governments that must continue to offer services, even as the tax revenues decline.

At Canaudit, we are committed to fighting overseas outsourcing. In the last two months we have increased our full time professional staff by 50 percent. While I cannot hire that security officer in Minneapolis now, I hope to be able to hire this outstanding person in January or February, as well as a person in May, and another one in August. We will fight outsourcing one job at a time. We will grow our company and our business by hiring

people who want to work, who want to excel, and who want economic prosperity for themselves, their families, and their communities. I encourage you and your organization to do the same. If you need staff, hire them. If you need consultants, put a clause in the contract that requires the consulting firm to source the work here in America, using legal residents and citizens. Do not let consultants source all or part of the staff overseas. Do not send your confidential information overseas simply to reduce costs. Each time you do either of these things, you are eliminating a job or part of a job right here at home. Remember, the next job lost could be yours.

There are a vast number of qualified professionals seeking employment in this country. Hire them, one by one. This article will be sent to 8,500 people. Some will pass it on. A few IIA, ISACA, and ISSA chapters may reprint it. As this article is passed along, maybe one person in ten will be in a position to hire someone. When you or your organization creates a new position, send me an email. I would like to publish some "good news" statistics in my next article.

Free Registrations for the IT AUDIT AND SECURITY BOOT CAMP

As I write this article, there are auditors and security officers who are unemployed and unable to get the Continuing Professional Education (CPE) credits they need to retain their professional designations (CIA, CISA, CPA, CMA, CA, CISSP, etc). To ensure that they do not lose them, we will reserve four spots in our IT Audit and Security Boot Camp, December 1 to 5, 2003 in the Washington DC area for those audit and security professionals who are between positions. To register for this class, please email Jennifer@canaudit.com. Include your name, address, phone number, and email address so we can contact you if you win. On November 3, 2003, she will draw four names to fill the spot. Each of these four people will receive a free registration (\$2,295 value) to the boot camp. The registration includes breakfast, lunch, and snacks throughout the day.

These Comments are mine

As always, the comments in this article are mine and mine alone! I value everyone's opinion and look forward to hearing yours. Please email your comments to Gordon@canaudit.com. I promise to answer them promptly and personally. If you would like to forward this article to your friends, I encourage you to do so. If you are not currently on our mail list and would like to receive a free subscription to the Canaudit Perspective, please email your name, address, phone number, and email address to me. I would like a chance to welcome you and will personally ensure that you are added to our subscription list.

If you are on the board of a chapter, the chapter may reprint this article in your newsletter at no cost. Please contact Jennifer@canaudit.com for permission to publish it.



Gordon Smith
President, CEO