



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

# **A Survey of IT Offshoring**

**Kelly K. Gieg  
GSEC Practical Assignment  
Version 1.4b**

**January 27, 2004**

© SANS Institute 2004, Author retains full rights.

“Offshoring” is a term that has been added to our lexicon in the past year or so to describe the practice of sending jobs from a country with a higher cost of living to a country with a lower cost of living and a therefore cheaper labor force. As the world economy becomes increasingly interdependent and as developing nations are embracing more capitalistic economies, Americans employed in the technology sector are starting to see jobs set sail for far away lands as companies move work offshore. In these tough economic times, this is a source of resentment, confusion and misunderstanding for many of America’s workers. For these reasons, it is difficult to find a source of unbiased information on the topic. Those who have a vested interest in presenting one side of the argument over the other often author the articles that have been written on offshoring. The goal of this paper is to strike a balance between both sides of the controversy and present the information in the most factual, unbiased manner possible.

This paper will begin by discussing the origins of IT offshoring. It is important to know from where the trend originated to understand where it is going. Next, this author will briefly touch upon the economics and the cultural aspects of the global economy with the intent of explaining why this trend will certainly continue. The final section will discuss what you, as a security professional, need to consider if you are ever in a position to administer offshore operations. Many of the principles that will be discussed are also applicable to onshore operations because they are firmly rooted in operational security best practices.

### **The origins of offshoring**

Despite the recent press, offshoring is nothing new for industrialized nations. Once mighty textile and steel industries have faded into the background of the American economy as these jobs have leaked from her borders. Consider the Levi Strauss Corporation, whose name is synonymous with denim products. Some twenty years ago, Levi Strauss had 63 sewing plants in North America, many of those in the United States. In January of 2003, Levi Strauss closed their last plant to move the final piece of their sewing operations to China. As competitors who used offshore labor expanded into the jean market, it became increasingly difficult for Levi Strauss to compete with onshore labor. Levi Strauss soon found out that they had to follow suit or risk perishing from the scene altogether.

Another industry that has embraced the practice of offshoring is the automobile industry. In fact, automakers have quietly been offshoring operations for years. Ford produces automobiles in Spain and England and GM has been producing cars in Germany for decades.

Interestingly, in the auto industry, jobs flow in both directions. The major Japanese and German automakers have setup offshore production facilities in the US to avoid anti-foreign sentiments as “buy American” campaigns have attempted to keep US dollars in the American economy. These countries have

found that offshoring their labor to our shores allows them to sell their product as a foreign-engineered product that is produced by American labor. This practice has proved to be very wise and as we shall see, it can help this companies avoid many of the public perception issues associated with sending labor overseas.

These industries are but a few of those employing offshore labor. Many other manufacturing industries moved overseas starting in the 1970's, but there was little outcry from the public except for those directly affected and from trade unions. After all, there are many economic benefits realized from offshoring. In developing nations labor is cheaper, governmental regulations are often more lax and raw materials may not need to be imported. These factors can help a company compete on price and quality leadership and free up capital for research and development efforts.

The American economy adapted to the loss of manufacturing jobs and shifted from a manufacturing to a services-based economy. This was viewed by most as a positive move, as many of those who would have been destined for manufacturing jobs in the past were now free to move into higher-paying white collar and skilled labor jobs. These jobs not only pay well, but they also came with better benefits and a higher standard of living.

Now, white-collar jobs are beginning to face the offshore challenge. The trend is in its seminal stages with most of the moves being in IT, but the impetus is carrying offshoring into all facets of our economy. Offshoring is projected to permeate industries as diverse as finance, creative design and management over the next ten years. Take Citibank and GE Finance as examples. Both companies have been quietly expanding into India for almost two decades now. Their precedence is significant though, because the financial services industry presently employs some 13 million people in mature industrial economies worldwide. Of those 13 million, 15 per cent or 2 million are expected to be shifted to offshore locations by 2008<sup>i</sup>.

### **Advantages of offshoring IT functions**

It is a business fact that labor and labor-related costs are the highest costs incurred by a company in the course of normal business operations. In the present economic climate, many companies with a global presence are looking for an "edge" that will allow them to reduce labor costs and to simultaneously maintain or increase worker productivity. As industrialized nations face mounting competition from developing nations, the practice of offshoring and nearshoring are becoming increasingly attractive alternatives to hiring and maintaining highly paid domestic labor.

India, China and Russia (among others) are churning out vast numbers very bright and capable technology workers. These countries have discovered that the initial investment in a technology infrastructure is far lower than the initial

investment in traditional asset-intensive industry (like manufacturing automobiles, for example). With a sense vigor and vision these nations have burst onto the tech scene in a very short time. At this time of the writing, India leads the pack as the prime location for offshore operations. Observe the following figures from Avanish Vashistha, senior adviser of NeoIT, a San Ramon, CA based offshore advisory firm. He estimates that 90 percent of outsourced code maintenance, help desk and desktop maintenance work is presently being sent to India with the remainder of the work in these fields being spread amongst the rest of the world<sup>ii</sup>.

It is not just the quantity and cost of labor that is available in these countries that is attractive to employers, it is also the quality. In many Asian and European cultures, there is an added emphasis on education, particularly in mathematics. Math is emphasized because the people of these countries know that math skills are always in demand, and having these skills puts one in the unique position of being in sought after in any country in the world regardless of cultural norms (unlike management skills, for example which are very culture specific). Those who have a firm command of these skills are at a great advantage in the technology industry, which draws heavily from engineering and scientific theory.

The American education system is more homogenized than that of many other countries. This has resulted in a greater level of educational parity among the average American citizen, but it has also perhaps pushed more American students to the center of the bell curve in terms of academic achievement. Those who advocate using offshore employees often point to the declining math scores of American students, in comparison to the rest of the world, to support the hiring of offshore workers for complex projects that require mathematic or engineering skills. This approach is insulting to many American tech workers, but as they say, "perception is reality", and the perception of those doing the hiring is of the most consequence.

It has also been stated by those whom employ offshore workers that the offshore workers are more willing to "get their hands dirty" doing the work that American developers rue. There is little doubt that many offshore workers are more willing to work long hours doing laborious work such as debugging source code than their American counterparts. This actually works well in the scheme of things. Spending hours pouring over somebody else's code trying to identify and rectify bugs is both time consuming and wearisome and not particularly well suited to the American mindset which emphasizes and rewards creative solutions over diligent labor and instant gratification over methodical solutions.

If you are interested in reading about what some of the top CEOs in America think about their offshore employees, go to the NASSCOM ([www.nasscom.com](http://www.nasscom.com)) website and click on the "Testimonials" link. Jack Welch of General Electric, John Chambers of CISCO Systems, Michael Dell of Dell Computers, Bill Gates of Microsoft and Larry Ellison of Oracle beam about their experiences with offshore operations in India. Each of the aforementioned speaks of their intent to further

expand operations in this direction based on the results they have achieved. Indeed, more than a quarter of the Fortune 500 companies are shifting parts of their back office operations to India as this paper is being written<sup>iii</sup>. This is some very strong evidence that these companies are realizing tangible benefits from this practice and intend to continue with offshoring practices in the future.

As a sidebar comment, the events of 9/11 lead to a brief pause in offshoring, but that trend has since reversed itself. There were many factors that went into the decision to forestall offshoring operations, but whatever those factors were, they are no longer perceived to be as significant as time goes on.

### **Issues to consider when offshoring**

As we have seen, there are many reasons to offshore from an economic and a quality standpoint, but there are of course, risks associated with the decision to offshore. The socioeconomic factors that lead to cheap labor are the very same factors that act as threat vectors to your company. Take into account the following issues:

#### **Loss of goodwill**

The reputation of the American corporation as an institution has weathered a beating over the past few years. The list of American companies that have been under assault in the press recently for illicit behavior includes some of the worlds most notable and prestigious companies. Names like Enron, Tyco, Arthur Anderson, Global Crossings and Adelphia have topped the list as fodder for media outlets eager to take up the cause against what they perceive as amoral corporate juggernauts.

An indirect but well publicized result of these scandals has been to help keep a weak economy down. The effects of the poor economy include mass layoffs (1,375,705 initial unemployment claims in 2002), benefits slashing and the wealth of many citizens drying up as the equity markets struggle. It is understandable why there is a rush to judgment when corporations release bad economic reports.

An announcement of a switch to an offshoring policy can turn out to be a PR nightmare for a company, particularly following a reduction in force of domestic employees. The media is quick to report on the pejorative aspects of a press release simply because good news doesn't illicit the same response from media consumers. For example, look at the January 17<sup>th</sup> press release from IBM where it was announced they would create 15,000 new jobs this year. While 4,500 of those jobs will be created in America, news outlets were quick to take note that majority of the new jobs would be created in China and India. While the net gain in jobs is positive for America, this author witnessed separate television, radio

and online reports that featured the number of jobs going overseas in the lead of the story, casting a pall on the positive economic news.

While it is easy to dismiss the effect of bad PR, it is important to not underestimate the importance of goodwill to a corporation. It is not easy to put a figure on goodwill, but the intangible value can manifest itself in subtle ways in the finances of a corporation. A loss of goodwill for a company can contribute to a reduction in consumer confidence, which can set in motion a chain of events that can ultimately result in loss of value for a public company. Because the primary mission of a corporation is to reward those who have invested in it by keeping share prices as high as possible, it is important to manage all variables that could affect stock value. To underscore this point, when goodwill can be valued, is carried as an asset on the balance sheets of a corporation in accordance with GAAP (Generally Accepted Accounting Principles).

When operations are moved offshore, public perception must be managed with vigorous information campaigns. Make sure investors and your consumers understand that these moves are part of a long-term strategic plan designed to make the company leaner and more competitive rather than being short-term myopic behaviors employed to cut costs quickly and easily. Also consider how employees, trade unions and other groups who have the media's ear will perceive these moves, as they will very likely be using the media as a conduit to express their views.

While managing goodwill and public perception, be also aware of the Sarbanes-Oxley Act of 2003. To be in compliance with the act, publicly traded companies will have to prove that the data being reported in financial statements is accurate and complete. A company's top officers will have to certify the reported numbers, and they can be held personally liable for damages if there is inaccurate information contained within the financial statements.

Sarbanes-Oxley ensures data integrity with the use of "controls". Controls are simply checks and balances designed by the company to ensure proper processes and procedures are in place to ensure accurate data flow. Controls must be implemented, tested and audited to prove that there is a minimum chance of error or manipulation of data. Poor or missing controls can appear as audit findings, which may be disclosed to the public. If investors or analysts perceive that there are weaknesses in your operations, it can affect public perceptions of how reliable your operations are. Having a strong operations security policy in place will go a long way towards meeting the expectations of the auditors. After all, the accounting data is processed on your systems and stored in your databases, so your role in maintaining the reputation of the company is probably much larger than you ever realized!

## **Human factors**

Taking people from completely different cultural backgrounds and geographic locations and expecting them to function harmoniously as one team can certainly prove to be a challenge. Many of these new teammates will never actually meet and will probably only communicate via email. There will likely be resistance to direct communication as different accents and dialogues can make an exchange uncomfortable for the parties involved. There is also the resentment factor to consider. Those who are working for the employer will often have feelings of hostility towards those who they perceive as stealing the jobs or their fallen comrades. Those feelings of hostility can impede normal communications flows, as emotional factors (metacommunication) can overshadow the message that is being delivered. Management must insist on proper professional decorum at all times to keep these feelings from being a disruption to the business process.

Sensitivity training is often employed by HR departments to help overcome cultural biases. Workers from different lands can and will offend each other quite inadvertently. This author works in a security organization that supports worldwide operations and can attest that business is done very differently in different parts of the world. The following observations are generalizations, but they can illustrate how differently business is done across cultures: Northern Europeans tend to be very direct in their dealings. They often have little tolerance for “small talk” and little sympathy when it comes to excuses for missed deadlines. Mediterranean workers are inclined to be more outgoing and conversational and often stress interpersonal relationships in solving problems. Asian cultures have a very intricate sense of honor and respect. For example, a worker with a lower status in the company should never question another worker with a higher status in the company, even if the question is in line with the policies of the company. It is important to know whom you are dealing with and treat them in the manner that they expect to reduce unnecessary friction.

Project managers need to remain very aware of these issues and they will be called upon to act as a liaison between teams when necessary. These managers should be assigned not just on the basis of technical or product knowledge but also on the merits of diplomatic acumen. Remember, these are not just “feel good” programs. A team that doesn’t mesh well can significantly affect productivity, which is a primary goal of offshoring operations.

The Interrelationships between the two sets of workers are important to manage, but it is important to also manage the expectations of the domestic employees who are removed from the offshore operations. Corporate finance officers should not hesitate to demonstrate the economics of the offshoring decision to the employees to increase buy-in. If the company is public, use the actual numbers that the decision to offshore was based upon. Explain why those who remain are still vital to continuing operations to maintain morale. People are far more inclined to support the process if they are shown that they can lose a percentage of jobs



through offshore attrition and remain competitive, or risk all by falling behind the competition.

When sending positions offshore, strive to adopt minimally invasive techniques. Auto parts maker TRW was able to time offshore hiring efforts with normal employee attrition. They reduced the prescribed headcount without firing a single employee by filling vacant positions with offshore labor as people retired or left the company on their own accord. Savvy observers will recognize that the net effect of this approach is still the loss of a job to an overseas operation, but those involved will have less desire to fight if their positions are not in immanent danger.

If an approach like the previous example is not feasible for your company, please take care to avoid blunders such as to have your employees train those who will be taking their jobs. Besides being the kind of tacky practice that will inevitably end up in the editorial pages, this practice is bad from a security standpoint. You never want to knowingly introduce motivation for an employee to sabotage training efforts or the operations at large. Use common sense and treat your workers with the respect that they are entitled to. Remember that it is not their fault that someone overseas can do their job for less money. Many of these employees are hard-working loyal employees that had no way of seeing this coming, and even if they did, they may have not had the wherewithal to do anything about it.

### **Loss of intellectual property and trade secrets**

Under this heading come several threats. One threat is the simple fact that offshore workers come in contact with your most intimate operations during the course of their normal work. As part of learning your operations, your offshore workers will gain knowledge that can be applied to other projects down the road. This is a positive thing if these projects are done on your behalf. On the other hand, your accumulated knowledge may be applied to solutions for other customers at a later date. Since most offshore workers are employed as contractors, there is the distinct possibility that this knowledge will be applied to competitors' solutions down the road. If you allow significant development of new projects offshore, be aware of this threat vector.

Some security professionals have also expressed fear that the offshore operation that you contract with may be able subcontract with smaller offshore operations to do your work without your knowledge. If you are not intimately involved with your offshore contractor, this scenario may not only be feasible, but in fact it can be quite plausible. Geographic distances and cultural differences can greatly diminish your scope of influence and control over your operations.

To take these scenarios even one-step further, your offshore workers could be involved in black market or espionage activities. Your product may be duplicated,

repackaged and sold on the black market while you are blissfully unaware. Whatever trade secrets you entrust could also end up in the hands of a competitor. The Chinese government has been accused of turning a blind eye to or supporting both of these activities. These allegations are given credibility because China doesn't have many laws in place to protect intellectual property and also because the Chinese government has been implicated on more than one occasion for sponsoring espionage programs against American interests<sup>iv</sup>. Despite these allegations, China is still considered to be "up and coming" in the offshore market.

One of the simplest measures that you can take to protect yourself is to always use reputable offshore employment agencies to contract out work. An agency with a clean track record of proven integrity will not engage in these practices. Take the time to investigate references. Good agencies are more than willing to provide a reference list, as it is a great source of advertising for them. Perhaps the best advice in this department is to keep core competencies at home where you can monitor activity more easily while sending maintenance and bug fixes over seas. The next section contains suggestions can help mitigate some of these risks.

## **Operational Security**

Most large American companies require the passing of stringent background checks of those who will have privileged access prior to job offers being extended. This is a good practice, but when your operations are sent overseas, how can you be sure of whom you have working for you? The short answer is that you can't. The reputable brokers in offshore services will conduct background screenings on your behalf but there is no way to be certain that the checks are thorough. Even if the investigators are diligent, it is still the case in many developing nations that the infrastructure needed to track all of its citizen's records is not sufficient to detect all unfavorable factors. This poses some significant risks in terms of personnel, but there are ways to mitigate the risks using the following operational security best practices:

- Use reputable offshore employment agencies that have locations in multiple countries. If the agency can satisfy the legal requirements of several nations, they are probably working with a sound business model.
- When made possible by local laws, require your offshore agency to vouch for their employees. Bind them with a contract stating that they will be liable for damages in the event of losses from a malicious employee's actions.
- Employ the "need to know" principle - only grant your users access to information or resources that are required for them to do their jobs. Grant the minimum level of access possible that allows them to work without undue interruption.
- Use the principle of "least privilege." This is similar to "need to know" but it relates to the rights that a user has as on the system opposed to user

permissions to an object. Again, grant the lowest level rights that you can without hampering the users' productivity. Error on the side of caution if you are unsure as to what rights are necessary. It is better to have a restrictive policy where permissions need to be added in as needed, rather than having a permissive policy where vulnerabilities may be exposed in an unpleasant manner.

- Require "separation of duties". Don't grant one user the authority to do a process start to finish, instead give each worker a "piece of the puzzle" to complete. It is even better to implement this procedure at the project level. Try and send only pieces of the project to the offshore facility so it is not apparent what is being created. Many experts relate this practice to encrypting the final result of your efforts. This process has been successfully employed by the military in developing highly sensitive national defense systems.
- Implement detective and corrective controls to detect and correct any misuse in or on the system. In this case, the best control for detection of misuse is to audit users frequently and thoroughly. Be aware of local privacy laws when auditing your workers, though. They can vary widely from nation to nation. Be sure that it is understood up front that activity will be audited on a regular basis and when warranted by a security concern. Corrective measures will vary based upon audit findings, but they will most certainly involve the removal of the offending party. Be sure written procedures are in place for the dismissal of users when the situation warrants it.
- Keep virus signatures and software patches up to date. Also, employ standard desktop images and enforce group policies in Windows machines using well-known security templates.
- Classify data and information based on impact to operations of the company. Clearly label sensitive data and information. Have policies in place that dictate proper handling of data that is classified at higher levels than "public" information.
- In a development shop, code reviews are critical to be sure that you are getting what you expect to get from your developers. If a full version of Flight Simulator can be hidden in Excel 97, it stands to reason that back doors, logic bombs, or other malicious code can be inserted into your source code fairly easily. Only allow trusted users the ability to check in revised code (least privilege principle).
- An interesting technique employed by this author's company is to instruct the offshore broker to not mention the name of the company until the hiring process is completed. This measure is designed provide a small measure of protection against those who would target a specific company for nefarious reasons.

### **Political situations (war, terrorist threat)**

The political infrastructure of many developing nations is often unstable when compared to the infrastructure of the industrialized nations. There are many gauges of risk, but one of the best sources is Chicago-based Aon Corp, who ranks countries based upon trade credit and political risk. Countries defined by Aon as high-risk are identified as such based upon the risks posed to the stability of the country due to economic, political, violence, and currency inconvertibility risks including war, terrorism, expropriation, and inability to transfer currency across borders. These risks can pose a serious challenge to business continuity efforts if they go unmitigated. Consider the following popular offshore locations and some issues that exist within their borders:

- India and Pakistan have gone to war three times since the two nations became independent from Great Britain in 1947. There remains a perpetual state of conflict that simmers in the border regions to this day. Since both nations have nuclear weapons, the result of another all out war could be catastrophic. Pakistan also has a history of hostility towards foreign businesses, even more so since the US has overthrown the Taliban in Afghanistan, as the Taliban enjoyed popular support in many regions of Pakistan.
- Malaysia and the Philippines have active terrorist organizations that are openly hostile to western interests. These organizations have demonstrated their willingness to kidnap Americans for ransom and they have also been implicated in bombings of locations that are frequented by western citizens.
- Russia has a wide-reaching and powerful organized crime syndicate that has filled in the void of a strong central government since the collapse of the Soviet Union. The stability of the country is based largely on the ability of president Vladimir Putin to maintain control of the country and on the uninterrupted flow of oil, which is Russia's key export.

The point here is that things can go wrong in ways not often considered by Americans who enjoy a mostly secure existence. We must be careful to not project our perceptions of the world onto another region that may have a vastly different reality. Be realistic, and look at all contingencies, even if they seem far-fetched. Transfer as much risk as possible with insurance and be sure to have contract specialists review insurance policies for exemptions that might bite you later. For example, many insurance policies don't cover claims that spawn from acts of war. Terrorism may be considered an act of war depending on the scenario and the policies of the insurance company in question.

It is critical when doing work in an offshore location to have stringent backup policies and well-planned storage locations. Backup media locations should be as far from any single point of failure as possible, but they should also be within reasonable distance to preclude major inconvenience when backups need to be restored. The facilities should also be hardened to the best extent possible. This means choosing buildings that are structurally superior and able to withstand

natural and man-made catastrophes. The locations should be revealed to only those who have a need to know, as a backup storage location could be a prime target to any terrorist who wanted to cause a major disruption in a company's ability to maintain continuity operations.

As an illustration, this author's company decided to use offshore operations in Chennai, India primarily because of Chennai's location on the Indian subcontinent. Chennai is located far from the border regions, where any potential war would be most likely to start. Another consideration is that Chennai is close to Singapore, which houses a large U.S. consulate and is a country that is friendly to western nation's interest. This author is not aware of where the backup media is housed, but it is known to be in an unmarked, remote storage facility that is rated at 1.5 times the required earthquake integrity standard.

### **Hidden Costs**

There are varying estimates of how much money can be saved by outsourcing, but many estimates predict at least a 50% savings in total costs when using Indian workers over American workers for comparable tasks. This figure may be changing, though. In the tradition of a market economy, wages are rising in India as the worker base becomes more skilled and as demand increases for their services. Being that this is a growth industry, some economists feel that India's wages could rise so fast that they could push much of the offshore labor market from India to China and Southeast Asia in the next decade (where wages remain lower). Those who have already committed to offshore operations in India may have to learn to "follow the leader" if they want to realize the maximum benefit from offshoring labor.

One also needs to account for the indirect variable costs associated with managing an operation that exists in another continent when considering the total cost of operations (TCO). Steve Andriole, a senior consultant with Cutter Consortium in Arlington, MA. and professor of MIS at Villanova University gives the following scenario: "When you send your people overseas to visit these sites often, your costs go from \$42 an hour to \$85 an hour." This differential is accounted for when travel costs and the costs of lost productivity (by the worker that must drop his/her daily tasks and go overseas for a few weeks) are looked at in amalgamation with the savings in lower wages. This calculation doesn't consider the associated but inevitable costs of "project creep" or run of the mill production problems that occur in every organization. He goes on to point out that "If you have to drop in 10 people from the states, and they spend a month or two there, guess what? You've just erased most of your cost savings"<sup>iv</sup>.

Dell Computers recently relocated its corporate support operations from India back to the United States (although at this writing, non-corporate support operations remain in India). Dell had many customer complaints ranging from communications issues to quality control and poor follow-up from techs.

Apparently, Dell found it was difficult to resolve these issues remotely, and they decided that it was more in their interests to scrap the project than to try and resolve the underlying issues. Failed projects always come at a high cost. The direct costs of moving operations can be easily measured. These costs include the cost of severance packages to the original American employees, the costs of moving the network infrastructure to *and back from* another country, the costs of training new employees (twice), recruiting costs for new American employees, etc., but the impact of lost confidence from unhappy corporate contracts are much harder to quantify. Time will tell, but this may end up being a major loss for Dell, if customers perceive that they were not committed to their best interests.

Anecdotally, this author has discussed this issue with others in the technology field and has found a sense of indignity towards Dell for this move. Comments by one technician were feelings that Dell is just moving back to America the profitable corporate support, but they are showing that they don't care about the home user by leaving these operations in India. Another tech noted that he would no longer recommend Dell to anyone in the office who wanted to purchase a home PC because of their offshoring stance. Instead, he recommended that anybody who wanted a new PC look to the smaller companies who produce and support computers with less overhead.

## **Conclusion**

As we have seen, the practice of offshoring is a complex issue. There are many factors to consider when making a decision of this magnitude. This paper was meant to get one thinking about the considerations of offshoring, but it was certainly not meant as an exhaustive checklist of how to offshore. There are services and trade organizations for that.

If embarking on an offshoring campaign, the process will include accountants, executives, PR departments, HR departments, network engineers, corporate training staff, IT security and others, depending on your particular industry. The project manager will have to call on the talents of many people to make the move successful.

This author began this paper with the intent of warning against using offshore operations. Intuitively, this practice sounds like a bad idea. Add to this the necessarily skeptical attitude of a security professional and all of the horror stories encountered in the community, and this author's feelings of dread rose quickly. However, in doing research for this practical and in talking with those involved in offshoring, this author realized that this kind of operation could be done with reasonable safety, but only with foresight and strong operational security. There are some major concerns when sending work to foreign countries, particularly in this hostile state of worldwide affairs, but when the company makes this kind of decision, it is up to all involved to make the directive work.

On a more hopeful note, this author believes that offshoring may be good for the economy in more ways than meet the eye. As the large companies find ways to cut the costs they need to survive, those who don't like this approach may decide to switch their support smaller and newer companies, which really are the foundation and the lifeblood of the American economy.

© SANS Institute 2004, Author retains full rights.

- 
- <sup>i</sup> Gentle, Chris. "The Cusp of a Revolution: How offshoring will transform the financial services industry". URL: <http://www.dc.com/Insights/research/financial/offshoring.asp> (27 Aug. 2003).
- <sup>ii</sup> Hoffman, Thomas and Thibodeau, Patrick. "There's More to Consider Than Cheaper Labor". Computerworld. 28 Apr. 2003. URL: <http://www.computerworld.com/printthis/2003/0,4814,80662,00.html> (28 Aug. 2003).
- <sup>iii</sup> hindustantimes.com, Friday, December 12, 2003. "Indian tech firms must focus on joint product development." URL: [http://www.nasscom.org/artdisplay.asp?Art\\_id=2231](http://www.nasscom.org/artdisplay.asp?Art_id=2231).
- <sup>iv</sup> Foot, David. "Offshoring IT jobs? Consider the risks, not just the rewards". 03 Jun. 2003. URL: [http://searchcio.techtarget.com/originalContent/0,289142,sid19\\_gci904410,00.html](http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci904410,00.html) (28 Aug. 2003).
- <sup>v</sup> "There is more to Consider Than Cheaper Labor".

Other References:

Hoffman, Allan. "CIOs on Offshoring." URL <http://technology.monster.com/articles/offshore/> (27 Aug. 2003).

Hayes, David. "BITS AND BYTES: Offshoring fad has a dark side". Kansas City.com. 26 Aug. 2003. URL: <http://kansascity.com/mld/kansascity/business/6616410.htm> (9 Sep. 2003).

Hoffman, Allan. "If Offshoring, Then What's Next for Techies?" URL: <http://technology.monster.com/articles/offifthen/> (27 Aug. 2003).

Nerney, Chris. "The Pros and Cons of Offshoring". 28 Jul. 2003. URL: <http://www.internetnews.com/comentary/article.php/2241131> (3 Sep. 2003).

Reynolds, Allison. "Aon maps high-risk areas for trade credit". (24 Jul. 2003) URL: <http://www.businessinsurance.com/cgi-bin/news.pl?newsId=2657>. (26, Aug. 2003).

Boel, Don, J.D. Edwards Senior Project Manager; 2003; Informal interview process.