Global Information Assurance Certification Paper

Global Information Assurance Certification
Security Essentials Certification Practical

Information Security Research Findings
Practical Option 1 Version 1.4b

The Outsourced Productivity Information Security Risk

K. Eric Mittler

November 5, 2004

Abstract

Many of your data protection security controls will be by-passed by your vendors if they feel pressured to do so by employees at your company, unless you specifically mitigate this risk. An outsourced vendor may have met the security standards like BS 7799 or ISO 17799, but your vendor is the paid to do what your company requests. For most businesses, productivity initiatives to gain revenue will trump perceived security burdens if the two are in conflict. This security vulnerability will make your company vulnerable to social engineering assaults. And the risks are higher when the outsourced vendor resides offshore. This paper discusses this problem, and risk mitigation that allow your business to maintain efficient productive relationships with vendors on outsourced projects. The observations are derived from review of published findings in print and on the Internet, and from the author's travels to United States and non-United States based outsourcing companies.

Audience

Those who are considering business plans that leverage outsourced and/or offshore companies for information technology work will benefit from reading this paper. While some of the conclusions here are applicable for non-information technology work, like manufacturing, the focus of this paper is on protecting the electronic data of your organization. In particular, the audience is corporate professionals at United States companies and this paper has a US focus, but the material here is practical for other nationalities.

Key Terms Glossary

The following terms from in this paper are used in this field of study, or may have alternate meaning in different contexts.

'7799

'7799 refers to either an ISO 17799 or BS 7799 standards based audit or control device.

Black Box Solution

A black box is a device that takes input and produces an output by unknown means. A black box solution is the result of using a black box.

BS 7799

BS 7799 is a security standard. ISO 17799, the current popular choice is based on this standard. Axel Bücker et al. assert in "Identity Management Design Guide with IBM Tivoli Identity Manager" that it is "the most widely known standard" and describe it nicely as "a single reference point for identifying a range of security controls, needed for most situations, where information systems are used in industry and commerce within large, medium, and small organizations."[1] BS 7799 provides guidelines to help you ensure quality security at your organization. It is an excellent device for security audits and is a standard that your company can achieve that can be used as an objective measure of comparison.

Contractor

A contactor is an individual who is employed by your company for a specific task and only for that task. The relation is based on a contract. After a duration or the completion of (or failure to complete) the task, the contractor's relationship with your company is terminated.

Defense in Depth

Eric Cole, in *Hackers Beware* defines defense in depth as the security "concept of having multiple mechanisms protecting a site."[2] This practice dictates the use of multiple layers of defense for valuable assets. Understanding that any one defense may not be adequate, having multiple different defenses is better than one. This concept is not new. One common example used to illustrate defense in depth is a medieval castle. Medieval castles were placed on hills to see the enemy coming, had walls to protect them, and were surrounded by motes with alligators (okay maybe no alligators in Medieval Europe).

Deprovisioning

Deprovisioning is the opposite of provisioning. It is the process of removing access (deleting or suspending accounts) on systems when an employee no longer needs the it. Accounts/access should always be revoked or "deprovisioned" when the owner of

the accounts leaves the company or related project.

ISO 17799

ISO 17799[3] is a security standard based on BS 7799. It provides lists and guides for ensuring comprehensive security practice at an organization. I concur with Mark Graff and Kenneth van Wyk in their book "Secure Coding: Principles & Practices" that of the "various standards…the ISO standard 17799, based on the British standard 7799, is a leader."[4]

Offshore

Offshore in the context of this paper means non-United States based. Employees that are based or located in other countries, or work for a company that is not US based, are offshore. This word may be ambiguous because from the perspective of the United States, Canadian, Mexican, Central American and South American countries share the shore but are considered offshore. Additionally, an employee may work for an Indian or Chinese company but may reside in the United States and work at a desk inside your corporate headquarters. Alternatively, an employee may be directly employed by your company but reside and work in a different country. You should consider that these employees are still "offshore" even though they may not reside or are based offshore. When categorizing employees for levels of trust, is smarter to use "outsourced" as a category than "offshore" because of this ambiguity.

Offshore Development Center

An offshore development center is a facility owned by your company or a vendor that is located outside of the United States, where information technology development occurs.

Outsource

Outsource is used as a verb to describe using a labor source other than full time employees of a company. That is, when a project uses contractors or vendors, that labor is outsourced labor. Additionally, when a process or machinery is not owned by the company, that process or machinery is considered outsourced. The term outsource is often confused with offshore. They mean very different things as an offshore employee may not be outsourced.

Non-Public Information (NPI)

For the purposes of this paper, non-public information (NPI) is data that your company may have about it's customers as defined in the US legislation Gramm-Leach-Bilely.[16] This information may be used by malfeasants to commit identity theft.

Provisioning

Provisioning is the act or process of proving access (i.e. accounts) to employees who work on company systems. Employees should be provisioned, so that they gain access to the information they need and no more.

Social Engineering

Social Engineering is type of assault on an information system where a malicious person uses subterfuge gain access to data to either steal from or damage your company or home. This may take the form of a bad guy working in plain sight, either taking advantage of lax security or innocent mistakes of employees to gain access to confidential data. Radha Gulati in the SANS paper "The Threat of Social Engineering and Your Defense Against It", nicely observes that there are two forms of social engineering: "technology based deception, and human based deception."[5] Gulati defines "technology based deception" as "deceiv(ing) the user into believing that he is interacting with the 'real' computer system and get him to provide confidential information," and human based deception as "taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked" to gain access. Additionally, social engineering can involve a malicious attacker taking advantage or your mistakes like going through your trash to find important data like passwords on post-it notes.

Trusted Network

A trusted network is the network of computers and devices of your company that is unavailable to the general public. The mechanisms for ensuring a trusted network will vary from firewalls to physical isolation.

Vendor

A vendor is a company that your company pays to do a service for your company. For the purpose of this paper, it is important to note that vendors may gain access to

sensitive information of your company.

Scope

The companies that you work for, and do business with, will (or already do) outsource work out to vendors that may reside outside the United States and outside of your direct information security controls. Some of these offshore outsourcing vendors are larger than your company and have better facilities than your company. Offshore development centers run by vendors can look exactly like your company, logos and all. They access systems in your trusted network. These locations may look like they have better security than your company. It seems like a security and productivity improvement to have your data processed at these vendor companies. And it very well may be. The marketing these vendors will present may be impressive, including independent security certifications (BS 7799 &/or ISO 17799).

You must remember that marketing and statements of security policy alone are not security. Information security professionals must follow up and validate the security practices of vendors when they have access to your systems. Your company must take the time to consider several novel risks. This paper focuses on the theme that your own company may pose a stronger risk to your data when you enter into a contract with an outsourced vendor than the vendor does. That is, while your security controls may be strong and the security controls of the vendor may be strong, the interaction itself creates vulnerability.

As a security consultant, I was asked to audit many outsourced offshore companies. This paper contains some observations and judgments based on those findings. The company I represented outsourced information processing and application development to offshore vendors. When I visited these vendors, I was generally impressed by the security practice and policy in place. In fact, the security was better than the company I represented in many ways. My ratings of these offshore vendors were highly favorable and in fact, I noted that much of information security services in the company I represented could be outsourced. But I noticed a key risk. The relationship between my company and offshore vendors allowed for introductions of vulnerabilities. It is an outsourced productivity information security risk.

The first hand research presented from my travels here does not represent a scientific study of all offshore vendors, (there is no double blind test or huge sample size). But rather this research serves an eyewitness description of potential security vulnerabilities that you can avoid, or exacerbate. The first hand observations described may seem obvious to security professionals, but perhaps have gone unnoticed by many.

I noticed in my offshore vendor visits that the customer service was better than what I am used to in my home country, the United States. The successful offshore companies I visited reside in countries that seem to have a culture of helpfulness and generosity. They are generally eager to please. These companies put huge emphasis on customer satisfaction. And during the economic downturns in the United States, these companies were very sensitive to customer retention. One way to attract customers and be more competitive was to demonstrate excellent security practice and present near perfect security policies.

I observed that when vendors are placed in the impossible position of loosing business because they must choose between be violating a security rule or not completing a job, the vendor logically chooses to violate the security rule. If a vendor does not complete the work at hand, there is a measurable failure, which may result in contract termination. If a vendor violates a security rule, the violation might not be noticed. The violation might be argued to be insignificant, or responsibility for the violation may be isolated or redirected. Security violations may be justified for the sake of productivity. And in fact, making an exception and bypassing a security control is the right thing to do when the risk of loosing business is less than the risk of data exposure. But if the bypassing of a security control is done covertly, quietly, without your company's knowledge, you have no control of the risk. Some violations may be against United States law.

I have observed that when dealing with vendors, all the security controls you put into place to protect your data will be bypassed by your vendors if they are ordered to do so by employees at your company. I conclude that as much attention and security control should be placed on your company's employees as your vendor employees.

The Problem

SANS teaches us that “vulnerability times threat equals risk” (Cole, Eric et al. Track 1 - SANS Security Essentials Version 2.2: Risk Management and Auditing)[6]. Several vulnerabilities may be created when outsourcing work that may weaken your company’s defenses to the constant security threats you deal with every day.

Threats

The threat of data exposure will depend on your company. Your company will have to determine the importance of its data to know what to protect and how to protect it. There are three high level data exposure threats to your company that this paper explores: ignorance or mistake, malicious insider activity and external assault.

Threat Factor One – Ignorance or Mistake

One of your employees will accidentally lose a disk or a laptop with sensitive data. An employee may post a message on a public web site too early or inappropriately. An employee may say something they should not say at a cocktail party. Accidents happen. I categorize this a threat (as opposed to a vulnerability) because ignorance and mistake can be represented as a constant force or actor attacking your company.

Threat Factor Two – Malicious Insider Activity

Your own employees may decide that they want to hurt you, or greed may overwhelm their lawfulness. A seemingly loyal employee, who passes your background checks, may initiate contact with an outside criminal group and may be blackmailed into hurting your company. The “2004 CSI/FBI Computer Crime and Security Survey”[7] shows that insider abuse of the network was second only to computer virus attacks. The August 2004 "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector"[8], shows that most security violations are non-technical and come from insiders leveraging simple non-technical means during regular business hours. I found this very persuasive and believe we should put the most energy into addressing this threat. But some insider attacks may be quite sophisticated. Obviously being on the inside of your trusted network provides a huge advantage to the attacker.

Threat Factor three – External Assault

An external assault is performed by non-employees who break through your physical and network controls (firewalls, barred windows, etc.), as opposed to the second threat

listed above where the assailant is already employed by you working inside your trusted network. One should consider the combination of this threat with the previous where an external assailant may try to gain employment at your or your vendor's company.

A common perception of an external information crime is the lone "nerd" teenage hacker, out for some kind of thrill. The current profile of information crime is changing. There are now organized criminal groups in other countries, disgruntled former employees, and even political or terrorist groups that are after your company's data. None of these persons may match the profile of a lone teenage nerd-hacker out for thrill. There are numerous assertions like those of Robert Graham, Chief Scientist of Internet Security Systems, that hackers are growing up to become "pros". An article based on an interview with Graham, on C|Net's News.com by Ong Boon Kiat, states "hackers are now far more coordinated" ("Hacking—Do the Pros Now Rule?" by Ong Boon Kiat http://news.com.com//2008-1082_3-5429687.html).[9] Kiat summarizes that "the motives (of hackers) behind the attack are changing…Graham detects a dangerous intent to profit financially from hacking."

It may seem paranoid to consider an organized criminal group wanting to attack your company, but the 21st century will show the maturing of information crime from the lone hacker to organize groups. It is not difficult to find reports and alerts to these organized efforts. Professor Phil Williams of the University of Pittsburgh asserts that "organized crime groups are using the Internet for major fraud and theft activities" and sites the logical growth of organized crime into high tech in his paper "Organized Crime and Cybercrime: Synergies, Trends, and Responses." Victor Sabadash of Crime-research.org asserts that "Computer crimes are becoming more and more transnational and organized."[11] Dr. Williams' article sites a few information crime examples that use high technology. But I assert that his examples are fundamentally non-technical in that the attacks do not involve breaking codes, buffer overflows, exploitation poor data validation etc. but are more in line with social engineering human factor deceptions. He sites several organized groups that work inside financial organizations to launder or steal money. Michael Vatis, Executive Director of Markle Foundation, Task Force on National Security in the Information Age, asserts that "the

threat of cyber-terrorism is real and growing" and sites a multitude of examples of recent cyber-assaults in his paper "Cyber Terrorism and Information Warfare: Government Perspective,"[12]. It is clear that this external threat is one that all security professionals must consider. If you are inviting in offshore non-full time employees to access your companies sensitive data, you have to be aware that there are malicious organized groups who will attempt to gain access through this new outsourced relationship.

Convergence of the Three Threat Factors

Chief Technical Officers spend extraordinary amounts of money on technical defenses. As their name implies, they are technical officers, and the information security departments often fall under them. But the studies sited have asserted that the most common threat (for financial organizations) is non-technical. This makes sense, as it's just easier for an employee to print out or copy data onto portable media from the inside than to break in from the outside. In most every US company I have seen, employees and contractors regularly take printouts and data media right out the front door. Often no technical control would defend the data as these employees are authorized to access it and Americans will not tolerate being searched.

Because your full time employees have more invested in the reputation, longevity and success of your company, contractors whether offshore or not pose a greater threat. Non-US citizen contractors who break the law and reside outside the United States are harder to catch and prosecute than US citizens residing the US. You expose your company to all three threats simultaneously when you create a situation where these contractors, working in your company's network, feeling cultural and productivity pressures from your employees, are coerced malicious groups. That triple threat may happen when your company outsources work to an offshore vendor. Engaging in an offshore outsourced relationship provides a new channel, a vulnerability, for these threats to emerge.

Vulnerabilities

Measuring your vulnerabilities will depend on the value of your data. If data exposure does not affect your business or break law, then the impact of data loss is negligible

and that vulnerability is not important. If the data describes your customers, then while loosing that data may not directly hurt your company, it may hurt your customers. That exposure may be illegal in many circumstances. It is critical that you categorize your data on a scale that reflects the cost of loss or public exposure, so that you know what controls should be in placed. By not categorizing your data you will waste time protecting the wrong data, not spend enough energy protecting critical data. And on the unfortunate event of exposure, you will not know the sensitivity of the data exposed.

Three factors, of concern to this thesis, converge to generate a significant vulnerability to your company. Your company's data or intellectual property may be exposed if these factors are not addressed. The factors are 1) the increased amount of confidential data your company has in electronic format, 2) the increased desire to be productive and cost effective, and 3) the increased exposure of your sensitive data and intellectual property to outsourced labor.

Vulnerability Factor One – Increased use of Information Systems

The United States is moving towards an information economy. Information is the primary asset or critical secondary asset of many companies. The importance of information systems of US companies continue to grow, even in times of slower economic growth. The population is increasingly aware of the importance and threat of information misuse, whether is it identity theft or Enron type information crime. Some companies are pure information brokers with very few physical assets of worth, and even "brick & mortar" manufacturing companies have increased information assets. The more systems and people that work on an information system, the more avenues there are for mistake or malice. And so there is increased vulnerability.

Vulnerability Factor Two – Productivity Pressure

Various pressures are forcing employees of US companies to be more productive. Many companies want to reduce labor costs by reducing head count and increasing productivity. They want to get one person to do the job of two. Employees that feel increased pressure to meet or exceed business goals will often feel restricted by security controls. There is a constant threat that employees will by-pass security controls in order to increase productivity.

Vulnerability Factor Three - Outsourcing

Competitive pressure forces companies to reduce cost. Companies are finding ways to cut payroll costs, reducing their full time staff, by outsourcing labor. Outsourcing companies themselves are "offshoring" labor to reduce cost. The explicit goal is to pay less for the same labor. That means that when companies outsource information technology labor, the people exposed to data are paid less than they were. Existing employees may feel threatened by this transformation and turn on their company. This presents vulnerability. And employees who are paid less are more susceptible to malicious activity for financial gain. Persons earning less may be less experienced. And less experienced persons may make more mistakes.

Risk

If you have no vulnerabilities, then you can save money addressing the threats. The threats of ignorance/mistake from internal sources and malicious activity from internal and external sources are always present. Typical United States companies have increased the use of information systems. They are facing increased productivity pressure and therefore use, or consider using outsourced and offshore labor. This is a vulnerability.

Are your employees likely to make mistakes, or are they not educated in information security? It is possible that your employees may damage your company's information systems. Are there organized groups who are trying to steal your sensitive data? Unfortunately, the research sited shows there are individuals and groups who wish to do damage or steal from your company for greed or political reasons. There is a threat. Therefore there is a risk.

SANS (http://www.sans.org) teaches us a multitude of ways to mitigate this risk. One can apply strict security controls on the process of sharing information with outsourced labor. Typically this takes the form of security audits and penetration tests. This paper presents several observations that illustrate some social factors and policy lapses that may not be revealed via standard audits. Network controls, intrusion detection systems, security policy, inspections with checklists are all part of a quality defense in depth strategy. The field observations below, in addition to checklist based

inspections, are this paper's suggested contribution to quality defense in depth and risk mitigation.

Field Observations

As a member of a security team at a large United States based financial services company, I perform technical security audits of offshore vendors. These offshore vendor audits consist of on-site interviews with offshore vendor staff and management, inspections of facilities, and accessing systems and devices for vulnerabilities.

The team's goal was to use a checklist form similar to one on the SANS/SCORE web site by B. E. Val Thiagarajan, "Information Security Management BS 7799 Audit Check List for SANS,"[13] which is derived from the BS 7799 standard. There are checks on policy to make sure the proper rules and procedures are in place to protect your data. There are checks for numerous physical security measures like fire suppression, and appropriate drop ceiling use. And there are checks for data quality controls like secure coding practice. While I cannot provide my list, as it belongs to my employer, the SANS checklist is an excellent resource and is in essence the same device I used.

Our checklist is not an end to itself. We summarize and expand on the findings. Just filling out a form is not enough. A mathematical sum of the checks of these forms can lead to fallacious conclusions. A professional objective judgment must be made for insightful conclusions. Some items are more important to your business than others and cannot be objectively weighed for all businesses. It is important to identify whether the controls listed in the forms that you deem important will be adhered to. This paper lists several observations that did not directly correspond to individual line items of our BS 7799 based checklist. They pointed to the theme that while the security controls were present, when given the choice between keeping or gaining business and enforcing security controls, a vendor will choose to keep or gain business.

If the controls examined by the use of a device like our checklist are adhered to, the vulnerabilities suggested by the following observations will not be problematic. But these observations suggest that just relying on these devices like checklists, vendor policies and procedures, and vendor (security) marketing is insufficient.

The observations presented generally focus on the social engineering type threats in response to the sited research that the new threats to the finance sector are insider non-technical and that these attacks are the easiest for organized groups to perform. In November 2004, based on a Gartner Group study, Munir Kotadia of C|Net's News.com asserts that "the greatest security risk…over the next 10 years will be...social engineering to bypass IT security defenses" ("Old scams pose the 'greatest security risk'" http://news.com.com/2100-7349_3-5435199.html).[14] The book "Security Warrior" by Anton Chuvaki and Cyrus Peikari provides an excellent description of a social engineering plan of attack. They present a ten point "Social Engineering Action Plan" that shows how an attacker would assault your company. They provide examples and describe how an assailant would use systemic iterative approaches to find weaknesses and exploit them. Beyond forms of passive attacks like eavesdropping your employees outside during smoking breaks, Chuvakin & Peikari define ten forms of active social engineering assault: "Intimidation", "Impersonation", "Blackmail", "Deception", "Flattery", "Befriending", "Authority", "Pressure", "Vanity", and "Sympathy" (this list from "Security Warrior" by Anton Chuvakin and Cyrus Peikari).[15] Radha Gulati's SANS paper (previously sited)[5] outlines eight different social engineering methods. Attackers will use each of these interactions with your employees to assault your systems. It is sobering to read their examples and think of your own, then relate them to the following vulnerability observations below.

Observation One – Poor Security Controls on VIPs

In order to get enter and exit one of the major offshore development centers, I had to check in at two different security guard posts. I had to list the electronic devices I carried and my bags were searched. I found it amusing that the guides hosting me apologized for this, when in fact, I was quite impressed to see how seriously they took the job of protecting my company's data.

A security specialist who was giving me the tour was happy to point out that Mr. H Ross Perot was there. He pointed over to a team of people. Indeed, they were from Perot Systems, but Mr. H Ross Perot was not there. I noted this as they passed through the same security checkpoint that impressed me before without any scrutiny,

and certainly no search.

I was shown policy saying that persons should be searched coming and going from the facility. An hour later when I left, I was let through without any questions or physical search. I volunteered to have my bags searched but the vendor insisted much to my surprise that I did not have to follow that security practice. I guess I was special. So my laptop with wireless card, and USB drive, made it right through their secure controls. And there was no check to see if a couple of their hard drives came along with me.

That offshore vendor knew that I was making recommendations as to whether to use their services or not. They wanted to make a good impression, so they avoided hassling me about physical security. Ironically, as a security analyst, I looked forward to a security check. I am not that important. One of the social engineering attacks sited is to assume authority. Given that they just gave me this "authority", I really doubt they would search someone pretending to be an authority while performing a social engineering attack. Perhaps they knew I was not a threat, and I was watched most the time. But I continually used my laptop and had enough time to use one of my many devices to install some malicious code. I was happy to see that this facility was removing USB ports from their machines.

My forms showed a checkmark on the section regarding physical security checkpoints. The vendors marketing material showed that they had security check points. I am not confident that they are as strong a defense as they appear.

Observation Two – Data Transfer Controls are not as Tight as They Seem

It was impressive to see a computer lab at an offshore facility with new computers and multiple physical controls to access it. Most of the computers did not have USB or serial ports. There were no CD burners or floppy drives. Managers monitored the printers. There seemed to be no way to get data on or off the computers that did not pass through their network policy enforcement devices.

We did a technical analysis of the network topology. We found a router that might be incorrectly used. Another offshore team, which was working for one of our

competitors, and so not accountable to my company, shared the router. We determined that it might not have been a serious security infraction in the way it was used. But the confidential data of my company and the data of this other company traveled across the same device in a shared closet. This sharing was done to save money.

I decided not to photograph the room with my digital camera, but I did take many other pictures of the facility. My digital camera and iPod both could easily copy confidential data. And the memory stick on my digital camera has a nice adaptor to act as an external hard drive. The people at the facility were impressed to see this technology, and most had no idea what they were. I believe that it did not occur to anyone how I could have used these devices to copy data and remove it from the facility. And certainly no one challenged me about it. There were several "no camera" signs that I decided not to take pictures of because I thought it would be rude. This is related to the first observation that they were poor the controls on VIPs.

Observation Three – The Vendor Black Box

Management at your company may rightly be concerned about security at vendor sites. I found that many managers care more about security at the vendor sites than they do at their own. More often than not, the staff at US companies I interviewed perceived the use of outsourced vendors as a "black box solution." Employees cared about security, but thought of security as something the company's security department took care of, and were satisfied with vendor marketing that their data was secure. The impression I came away with was that employees did not feel security was a personal responsibility.

The primary concern of my company's employees was getting the job done in a profitable (cost effective) and expeditious manner. Vendors are seen as tool to get the work done, less as a human resource to manage, and more as a well defined quality controlled tool, like a fork lift or cargo ship. But there are not the standards and quality controls on offshore information processing vendors like there are on domestic manufacturing of cars or fork-lifts.

If employees of the offshore outsourced vendors are thought of as a black box,

they will have no insights as to what is going on in your company. That isolation will lead to mistakes and lower productivity.

The lesson is that any security audit of an outsourced solution must include an examination of your own company. If your employees think of a vendor as a black box, you are vulnerable.

Observation Four – You Don't Know Who is Working on Your Project

Not knowing who has access to your company's data is an unacceptable vulnerability. When your company has a project dealing with its intellectual property or sensitive data, your company must know who is working on it. You may be required by US law to have this knowledge. Will vendor employees working on your project have access to customer information, non-public information (NPI) or other confidential data? Because you are doing the base security work, you will ensure that people will have to authenticate and be authorized to access this data. You will, of course, audit system access. But this takes time. What happens when the project is running behind schedule?

As stated before, one of the attractions of outsourced work is that your vendor can appears a "black box" solution. That is, you put money in, you do not know what goes on inside, and you get a product/solution coming out. In fact, many outsourcing vendors present themselves this way. The idea is that the vendor commits under contract to finish the work. And one of the ways the vendor can ensure success is to put as many people as needed on the project or even outsource again. That means, in the course of your project's life-time, it is possible that you may not know who is working on your project and is accessing your data.

Many countries where vendors reside do not have an authoritative identification system. Passports or driver's licenses may not be reliable forms of identification. They will not have Social Security Numbers. Not having a common ID means that a vendor will have difficulties with background checks, and may allow criminals to work for them.

I observed that most of the projects I have consulted on have had resource problems, scheduling errors or feature creep. This is to be expected and often it is not

of consequence. But these errors will create pressure on the managers of the project. When this occurs, one of the first solutions examined is to bring more people on to the project. Because of the time pressures, the project managers will not want to "waste time" setting up new accounts for new people. And I observed that when outsourced vendors are perceived as a black box solution, employees at your company will not care if your vendor employees share accounts. If the vendor does observe the security controls, the vendor will present the problem back to your company: either we violate security controls and get the job done expeditiously, or wait until the security procedures can be followed and let the project time line lapse more. The vendor may look bad doing so.

I found an account called "pmeta" on a UNIX system. It seems on the surface to belong to a person called P. Meta. On later examination, I found that it was in fact a generic account belonging to "a temp" -- pmeta spelled backwards. When I challenged the responsible manager at my company about this, I was told that it took too long to provision accounts. He thought it better to have this account that his many temporary workers could share. Unfortunately, there was no desire from the senior management to discipline this problematic manager. Additionally, there were discussions about firing the contracting firm for security violations. I felt that my company was quick to blame the vendor for what was obviously (to me) our fault.

Observation Five – When Things Go Wrong at the Vendor Site, Do You Know?

Again the marketing pressures on the vendor will provide incentive to keep secret any security lapses. Your contract with the vendor may force the vendor to disclose security breaches, but these may only relate to breaches that effect your information and not those of other companies that do business with that vendor. Recall the shared router mentioned above. My company would never know if a sniffer (a device that monitors and can copy network traffic) was attached to it by a malicious insider at the other company.

Natives of many of the countries I met with were, at a minimum, fearful of the governmental authorities. In one country, when I stood too close to an army solider or

looked at a police officer, I was quickly ushered away by my minders. When I questioned why, I was informed that it was just best not to deal with the police and it was implied that it was dangerous to interact with the army soldier. In another country, it was just given that interactions with the police meant the potential of jail time or bribery at a minimum. When I asked what effect this perception of authority had on the company, I did not receive a satisfactory answer. I say this not to be xenophobic, but rather to point out that you cannot assume the same United States cultural notion of law and respect for governmental authorities in the countries that have offshore development centers.

I was left with the impression that reporting crime, or security violations, to authorities was not the same as it is in the United States. It may not be fair to make a correlation between the way people adhere to traffic rules when they drive and adherence to security policy; but it is not difficult to infer. I was unlucky enough to witness two different horrific traffic accidents with multiple fatalities on my travels during my security audits. It was immediately apparent that both were a result of failure to observe basic traffic rules. And for both accidents, with dead bodies, there were no police or emergency vehicles present. While this may have no bearing on offshore vendor employees reporting security violations, it struck me as a theme. If an employee is willing to work for so little, and there is so much competition for work, will the employee have the any interest to blow the whistle when they witness a security violation? What about if it involves a death? If that employee has more incentive to be productive than adhere to security policy, and security authorities are seen as dangerous, erratic, bribable and corrupt, then there may be a culture where obedience to security rules is not important. In such a culture, offshore vendor employees may not tell you when there is a security violation.

Observation Six – When The Worst Happens, Who Takes Responsibility?

When your company outsources work, it is looking for someone else to provide the solution. When the project succeeds, and your vendor performs well, the employees at your company will take the credit. But the nature of the desire to outsource work is

that when something goes wrong, we naturally want to blame the vendor for the failure. I continue to observe this daily. And while failures in projects may be the fault of the vendor, your company must be responsible for oversight of data, especially non-public information (NPI) as defined by the Gramm-Leach-Bliley Act [16]. A security audit of the vendor and vendor site will not expose the failures of your company to oversee work.

The use of the "pmeta" account (described in observation three) is a good example of misplaced responsibility. The manager in this case who violated security policy (account sharing and the use of generic accounts) was rewarded for his behavior. If something had gone wrong (thankfully nothing did), and a contractor used this account for malice, we would have had a difficult time proving who did it because several people could have used the account. And when this policy was violated, there was desire to blame the vendor.

If your vendor is in another country, do you know what legal redress you have if something goes wrong? You should have a plan.

Observation Seven – Language / Communication Problems

Communicating the issues of information technology is difficult enough when employees are in the same room. When working across time zones and thousands of miles, there are obvious problems of dealing with telephones, email, faxes, and video conferences.

From the perspective of a United States company trying to find a vendor in another country, it is appealing to work with a vendor from a country whose first or unifying language is English. I have found that there are sometimes more difficulties between two countries that both speak English than between countries that speak different languages. When the countries speak different languages, there is an expectation of communication difficulties. When both countries speak the same language, communication difficulties may not be expected or obvious. This may be a particular difficulty when dealing with legal policy, or communicating the security needs that may be in conflict with productivity.

For example, I noticed, when reviewing security policy at several English speaking offshore vendors, that they used the word "shall" when comparable US policies used

the word “must”. For example, “employees must wash their hands after sneezing” versus “employees shall wash their hands after sneezing.” I attribute this to the differences between British English and American English. In a non-scientific poll of my friends in England and India compared to my friends who grew up in Texas, Massachusetts and California, I found that all the Americans inferred a stronger negative consequence to the use of the word “must” and thought the word “shall” might not have as severe negative consequence. The offshore vendor policy may use the word “shall” and your US company employees may not respect those policies or absorb the negative consequence of violation. Additionally, your employees who are time pressured (vulnerability factor two above) and are already predisposed to think of an offshore, outsourced solution as a black box (previous observation three above) a word like “shall” may look like optional behavior. This may seem subtle and inconsequential, but these communication misunderstandings can multiply, and lead to the first threat of mistake or ignorance when combined with different uses of hand, and head gestures, idioms and corporate jargon.

The vendor policy will pass a '7799 type audit using any language, but it may not be a security control for your employees. None of these subtle linguistic issues will show up on a cursory security audit, especially when performed by technologists who are less versed in linguistics.

Observation Eight – A Culture of “Yes”

I am very impressed by the can do attitude of the offshore vendors I have visited. In one country, I tried to count the number of times I heard the word “no” in regards to statements of what could be provided to me. After talking to several dozen people at offshore vendor locations, the count was less than ten. It seems like everything is possible at a fraction of the price it would cost in the United States.

Obviously not everything is possible at a reduced price, even with lower labor costs. When the reality that a project cannot meet expectations or deadlines, a vendor will be challenged to put more people on the project, and cut corners. With a culture of yes, your company may not learn that an endeavor is problematic until it is too late. Some of those cut corners will be violations of security policy, best practice or US law.

Summary of Observations

The goal of my audits was to address each item of a list similar to the SANS BS 7799 based security audit form sited.[13] These observations presented did not directly fit into the audit, but appear as notes or explanations of failures. Many executives are quick to look at summaries and are not inclined, or have the time, to review the detailed notes. In general, the observations listed in this paper represent failures of vendors to meet quality security policy for working with confidential data (in particular working with United States financial institutions). At a high level, one might discern that an outsourced vendor solution will protect data. When the vendor site is on the other side of the planet, executive decision makers will have to rely more on secondary sources of security assessment. The theme of the observations will not be addressed by only relying on vendor marketing, legal contracts and checking security audit forms. They are addressed by on location audits and communication with staff at your company and at the outsourced vendor site. You must prepare for the special tensions of productivity pressure on outsourced work in advance. These vulnerability observations

1. Poor Security Controls on VIPs
2. Data Transfer Controls Are Not As Tight As They Seem
3. The Vendor Black Box
4. You Don't Know Who Is Working On Your Project
5. When Things Go Wrong At The Vendor Site, Do You Know?
6. When The Worst Happens, Who Really Takes Responsibility?
7. Language / Communication Problems
8. A Culture of "Yes"

and others you find when you visit vendor sites, will alert you to the risks when your company pressures vendors to be more productive.

Risk Mitigation

There are ways to mitigate the problems of security policy violation resulting from the productivity pressures in outsourced work. You must address security issues for both vendor and internal employees. First, you must have educational programs, rules, actions and consequences applied to your company before you engage your vendor.

And second, you must have rules and legal agreements applied to your vendors. Your first step is to determine your risk. How vulnerable are you?

Accounts and Data Access

One key defense must be auditing system access so it is apparent who can access your information, and who can improperly expose it. When employees can access sensitive data, you must follow these rules:

1. You must know what account has access to what data
2. You must know who has access to what account,
3. You must require that accounts not be shared.

Not knowing who can access your data is an extreme vulnerability. This vulnerability is not new. Companies of previous centuries have had security breaches due to technical failure, ignorance of employees or sabotage. The difference now, besides scale and speed, is offshore outsourced work allows for exposure of your companies data instantaneously on the opposite side of the world. If you know who has access to your data you are safer than if you do not. But knowing this is a challenge.

There are several steps you can take to give your company this knowledge. These are 1) categorize your data; 2) have a system for provisioning and deprovisioning access, 3) establishing a chain of responsibility, and 4) review access. By policy and practice, implementing each of these will give you the tools to mitigate the risks presented by the outsourced productivity security risk observations presented in this paper.

1. Categorize Data

As stated above, you will not know if you are vulnerable if you do not know the value of your data. For each project, the owners should categorize the data there so that it is known in advance what audiences should be able to access it.

2. Provisioning and Deprovisioning

Your company must deprovision and provision appropriately and expeditiously. When managers review accounts of outsourced (and full time) employees, the managers should be able to quickly grant and revoke access to systems. When dealing with

employees paid by the hour, speed is critical. Expeditious account creation and deletion is key nexus between productivity and security. If it takes too long to create (or delete) accounts, employees will either not be productive or by-pass security measures (i.e. share accounts) to be productive.

3. Chain of Responsibility

You must implement a chain of responsibility for system access. It is impossible for one person or account provisioning group to know what access every person in an organization should have. Each full time manager (full time or vendor) must be held accountable for knowing what accounts are owned by their direct reports. If a manager is unavailable the next person higher in the chain of responsibility must act as a backup. And each manager's manager should be held responsible for ensuring that all managers review access of their direct reports. This forms a chain of responsibility all the way up to the CEO.

If an employee misuses an account, the full time manager must be disciplined. This should include employment termination if their employee exposes confidential data. But there should be a carrot to this stick. If managers can demonstrate that they know the access of their direct report, they should receive a monetary bonus. Your company should market the fact it has this quality control.

4. Review Access

It will not be enough if you just categorize data and provision access properly. You should have an external party review security related processes to ensure they are being done properly. This external auditing group checks that the chain of responsibility exists.

Summary

All of these points are actions that you take internally in your company and are not requirements of your outsourced vendor. Adherence to security controls that even approach those of BS 7799 or ISO 17799 will encourage each of these risk mitigation practices. But each of these actions is a burden on your staff. You should recognize this extra work and prepare for it in advance of your outsourced engagement, and do not just rely on the vendor's security controls.

Vendor Requirements

You have categorized your data; you have a system for provisioning accounts; you have a chain of responsibility; and you review access. Next you must make sure your relationship with your vendor is consistent with these practices. Vendor employees must know your data categorizations, their accounts must be provisioned by your mechanisms, and the vendor employees must fall into the chain of responsibility of your company. And, of course, your security auditors must be able to examine these mechanisms in the off site vendor location regularly. Before you enter into a relationship with your vendor, you should have these mechanisms codified in legal contracts with specified consequences.

It may be the case that working with the vendor is the only way to accomplish a task to remain competitive. You should recognize that your company may become so reliant on the vendor that it may impossible to terminate a vendor contract if there is a security policy violation. That means that you must have in the contract legal mechanisms for your company to have compensation if there is a violation. And at a minimum, you should have non-disclosure agreements. It may be possible to make individuals at the vendor site personally responsible for the security controls. If there is a security violation at the vendor site, the responsible individual must be held accountable.

I would strongly recommend that you defend your vendor too. It should be clear that when persons at your company requests that your vendor violate security practice that your vendor can safely say no without fear of reprisal. Be cognizant of the "culture of yes." Make sure your contract with your vendor both defends the vendor if the vendor says no to sharing accounts, and punishes the executives and managers at the vendor company if the vendor violates security policy. The vendor should have a channel into your company's security staff to document such security violation requests. Make it easy for the vendor to report violations. This practice will be the key to mitigating the outsourced productivity security risk.

Whenever possible, let the vendor work with fake data and not real data. "Scrub" your data. That is, if real data is not needed to prove the system works, do not use it.

Internal Actions & Controls

Many companies will seek vendors that have a '7799 (BS 7799 & ISO 17799) type of certification. It is not cost effective often to apply those same controls internally. As stated, you will need to have provisioning processes in place that control system access. Your company has (or should have) security policy, appropriate data transfer controls (firewalls), intrusion and inappropriate use detection systems. These will mitigate the risk from all the stated observations, but you can go a few steps further and internally address the specific issues of productivity pressure on outsourced vendors. You should be aware that your employees may be the cause of security issues in your new relationships with offshore vendors. There are some simple steps you can do to address these.

Training - Cultural Sensitivity

We know that there are very different business styles in Manhattan's Wall Street compared with Cupertino. These styles are based on culture and the local way of life. One should expect bigger differences between styles of business in cities that are in different countries.

Toni Bowers in *TechRepublic* (http://techrepublic.com) advises us to "think of cross-cultural outsourcing as a marriage."[17] Both sides must strive for good communication for a healthy relationship. As observed, many of the problems working with offshore employees come down to communication difficulties. And communication difficulties can make expose you to security risk. These can be anticipated. Knowing that there may be problems ahead of time is half the battle. You should take efforts to have materials, documents, and videos available for your employees that educate them about the culture of the other countries you work with. It is not sufficient to know that people at the offshore site are learning American mannerisms. Americans must learn about the cultures of the employees at other countries. For example, employees should know what it means to shake hands, make arm gestures, shake your head in particular ways, or bow. Just knowing a few of these differences will alert your US employees to the notion that there may be other cultural and communication differences. There are wonderful secondary gains in productivity

and personal growth to this security focused practice.

Training - Vendor Relations

Internal employees must know the rules for engagement with offshore vendors. Before your company works with the vendors, you must know what information the vendor can access. Determining this on the fly will leave you vulnerable to data exposure. Internal employees must, at minimum, sign legal documents that specify what information your internal employees can share with vendors. Your employees should have training to know what data they can share and best practices for managing vendor relations, deadlines and budgets. This will have both security and productivity returns.

Training - Security Awareness

If your employees know that when they force vendors to violate security policy the vendors will report it, your employees will be dissuaded from doing so. Your employees have a vested interest in the success of your company. By providing training, your employees will see how they can contribute to the defense of the company. The observations of this paper, and your own, can form entertaining, attention grabbing material for the students of these training sessions. You should hold classes, lectures (stream them via your intranet), send email, create an internal web site, and show movies (like the 1992 "Sneakers" http://www.imdb.com/title/tt0105435/). Making your employees aware of the threats and vulnerabilities is the best way to mitigate the social engineering attacks.

Reward Good Security Practice - Punish Security Violation

You may need to be creative to generate rewards for good secure vendor relations. Most employees respond financial reward. If adhering to good security practice and attending training is a part of each employee's advancement review for promotion and pay increase, you will see positive results.

Unfortunately, there will be some who will still violate security rules. You must prepare for this in advance. Before employees at your company enter into relationships with outsourced vendors, they must sign legal papers that spell out the consequences of security policy violation, which should include termination. This was not done in the case of the “pmeta” account and so there was no corrective action

taken.

Learn from Observations & Incidents

A part of any security group's practice should be to quantify, review and make judgements on security incidents. The '7799 standards promote this process. In addition to reviewing security incidents, adding the review of security vulnerabilities observed into this process will be of value. I highly concur with Richard Forno & Kenneth R van Wyk's statement in their book *Incident Response* that "all too often, when organizations develop information security programs, they treat security issues as a simple 'check-box' on the list of required corporate functions." [18] They point out the dangers of this approach and argue for systemic continuing processes for security practice. They discuss mechanics of individual system security measures like intrusion detection systems, incident response reports, and log monitoring systems. These are tools for the foundations of strong risk mitigation and can form a continuing report to executives about the state of your company's security. I would suggest adding observations like those sited in this paper to guide future iterations of vulnerability assessments and security awareness training.

Insurance

If you have valuable assets, you should insure them against lost. Having your data stolen, made unavailable or lost because of malice or mistake in your relationship with an offshore vendor can be insured. Insurance companies have been analyzing risk and placing a monetary value on intellectual property for centuries. These companies may be an excellent resource for determining your risk exposure. Bruce Schneier in his article in *Information Security* (http://infosecuritymag.techtarget.com) goes so far as to predict that "the insurance industry will subsume the computer security industry."[19] Schneier claims that "when it comes time to calculate the premium, the details of network security become checkboxes." I disagree with the notion that security is just "checkboxes" in part. Relying on checklists alone is a mistake, because we know that the security controls they represent will be bypassed when productivity pressures are too strong. Schneier concludes that "the insurance industry will sell everyone anti-hacking policies" and I concur, and recommend insurance in the course of pursuing

offshore vendor relations.

Conclusion: Anticipate the Observed Vulnerabilities & Share Stories

The threats and vulnerabilities discussed are nothing new. But given the new nature of work in the United States, exposing sensitive data by mistake or malice will be easier if precautions are not taken. Check lists, and reviews are excellent controls. But I find that a regular systemic process of sharing your observations and anecdotes is extremely effective. People listen and learn from the stories better than dry summaries from lists. And they invite participation. If an executive at your company is told in advance when visiting a vendor site to observe whether the security controls apply to her perhaps your executive may be more vigilant. If your managers do not see vendors as a black box, they will naturally have a greater insight to the remote exposure of your company's data at the offshore site. If your project owners expect a "culture of yes" or know that individuals in different parts of the world may have different emotional responses to legal authorities, your projects will be more culturally aware and secure.

You must defend your vendors. If your vendor has nothing to gain from secure practice after they have signed a contract with you, and everything to loose by not pleasing your project managers, they will violate security policy. This is especially true when your employees pressure them to do so. You must provide a mechanism for your vendors to report requests for security violations.

Outsourced vendors know all the checklists and auditing forms. These companies may have better security than yours. Look between the lines of the checklists, visit the offshore vendor sites, and observe for yourself. Make these observations more than end notes and bring them to the attention of the decision makers. If you share these observations with your vendors, they will know that you care about security and will be on guard, will defend your data, even when employees of your company insist on policy violation that may expose your data for the sake of productivity gains.

References

[1] Bücker, Axel and Camp, Andrew and Cohen, Rick and Edwards, David and Penman, Collin and Sant'ana, Thomas. (2003). Identity Management Design Guide with IBM Tivoli Identity Manager. IBM Press. ISBN: 0-7384-5332-3

[2] Cole, Eric. (2002) Hackers Beware. New Riders Publishing. 18.

[3] ISO/IEC 17799:2000(E). (2000). Information technology – Code of practice for information security management. Switzerland. ISO copyright office.

[4] Graff, Mark G. and van Wyk, Kenneth R. (2003). Secure Coding: Principles & Practices. O'Reilly. 157.

[5] Gulati, Radha. (October 31, 2003) "The Threat of Social Engineering and Your Defense Against It" http://www.sans.org/rr/papers/index.php?id=1232. 1.

[6] Cole, Eric and Fossen, Jason and Northcutt, Stephen and Pomeranz, Hal. (2004). Track 1 - SANS Security Essentials Version 2.2: Risk Management and Auditing. SANS Institute. 347.

[7] Gordon, Lawrence A. and Loeb, Martin P. and Lucyshyn, William and Richardson, Robert. (2004). "2004 CSI/FBI Computer Crime and Security Survey", Computer Security Institute. http://gocsi.com/forms/fbi/pdf.jhtml

[8] Randazzo, Marisa and Keeny, Michelle et al. (August 2004). "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector". Carnegie Mellon Software Engineering Institute. http://www.secretservice.gov/ntac/its_report_040820.pdf

[9] Kiat, Ong Boon. (October 28, 2004). "Hacking—Do the Pros Now Rule?" http://news.com.com/Hacking--do+the+pros+now+rule/2008-1082_3-5429687.html

[10] Williams, Phil. (August 2001). "Organized Crime and Cybercrime: Synergies, Trends, and Responses". http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

[11] Sabadash, Victor. (2004). "IT and Organized Crime". http://www.crime-research.org/library/sabad02_2004.html

[12] Vatis, Michael. (2001). "Cyber Terrorism and Information Warfare: Government Perspective". http://www.terrorismcentral.com/Library/Teasers/vatis.html

[13] Val Thiagarajan, B.E. (August 2003). "Information Security Management BS 7799 Audit Check List for SANS". http://www.sans.org/score/ISO_17799checklist.php

[14] Kotadia, Munir. (November 1, 2004). "Old scams pose the 'greatest security risk'". *C|Net News.com*. http://news.com.com/2100-7349_3-5435199.html

[15] Chuvakin, Anton & Peikari, Cyrus. (2004). Security Warrior. O'Reilly. 208-210.

[16] "Information Regarding the Gramm-Leach-Bliley Act of 1999". (November 1999). Web Site of the U.S. Senate Committee on Banking, Housing and Urban Affairs. http://banking.senate.gov/conf/

[17] Bowers, Toni. (April 2004). "Cross-cultural outsourcing requires planning and sensitivity" *TechRepublic*. http://techrepublic.com.com/5100-6314_11-5197010.html

[18] Forno , Richard & van Wyk, Kenneth R. (2001). Incident Response. O'Reilly.

[19] Schneier, Bruce. (February 2001). “Schneier On Security: The Insurance Takeover”. *Information Security Magazine*. http://infosecuritymag.techtarget.com/articles/february01/columns_sos.shtml