

Overseas Outsourcing: a look at the security risks

Overseas outsourcing can save money. However, that money savings comes with a price tag attached. It is critical that CIOs are aware of concerns and complexities that are involved prior to engaging in overseas outsourcing.

Philip Alexander
October 17, 2007

Overseas outsourcing can often help companies realize substantial cost savings by sending certain functions overseas, where labor costs are a fraction of those here in the United States. However, there is more to consider than just the lower labor costs of employees in India versus their domestic counterparts. In this day and age of heightened security sensitivity, it's important to make sure that in addition to going after cheap labor, you're not buying yourself a slew of security exposures as well.

The decision on whether or not to outsource should not rest solely with the CFO. The chief security and compliance officers should also be involved because of the many security- and regulatory-related issues involved with offshore outsourcing.

Data risk exposures

There are two major issues to consider when addressing overseas security and data risk. The first is granting offshore engineers access to computer systems located within your company's network. Are you monitoring the activities of the overseas engineers? If the work that's being sent offshore is project-based, are you ensuring that access is removed when the project is completed? Do you have security professionals monitoring the activities of the offshore engineers? While all of these activities are critical, they add both complexity and cost to IT off-shoring projects.

It is also important to review what type of work is safe to send offshore. For instance, outsourcing production support overseas entails a high degree of risk. Engineers providing production support generally need to have highly privileged access in order to provide said support. Such access also simplifies illegal activities such as data theft and industrial espionage. Give a clever engineer enough access, and he or she can not only steal data from you, but they can also thwart any monitoring software designed to detect such activities.

You should consider projects that don't entail sending sensitive customer information offshore, or granting remote access to your internal network. Software development doesn't require providing sensitive customer data offshore. The development work can be performed offshore, then the code can be securely transmitted to your company. You may consider creating a special offshore/development segment of your network allowing your offshore engineers to work, while not providing access to the rest of your internal systems.

Think about the type of information that you're sending overseas. Will it include sensitive information such as medical records, Social Security numbers or tax returns? While privacy laws for electronic data are relatively new here, they are almost nonexistent in many foreign countries. Even where there are legal prohibitions to data theft, the actual number of prosecutions are minimal. Simply put, there just isn't too much risk in committing data theft in many overseas countries, particularly if the victims are foreigners, (in this context, that would be you and me).

A cornerstone of effective data security is to provide information on a need-to-know basis. This applies to off-shoring as well. Closely consider what information your offshore workforce needs to access. Can you substitute a customer identification number for a Social Security number? If so, that would reduce the risk to both your customers and yourself. Look for similar opportunities, as this can greatly reduce your data risk exposures.

Background checks

Much of the new-hire vetting that's commonplace with background checks performed here in the United States just can't be done in many foreign countries. For example, India just doesn't have the capabilities to perform what would be considered a thorough background check by American standards. In addition, drug testing is generally not done as part of a background check in India. The exception is checks done when applying for an Indian passport. So your company can actually benefit from government background checks by contractually mandating that all employees handling your company's data have an Indian passport.

Regulations

With the rash of highly publicized data breaches, 39 states now have their own disclosure laws mandating that companies inform customers in the event of either an actual or suspected security breach. This applies to data breaches that occur overseas if you send sensitive customer data offshore.

In fact, many states are becoming so concerned with the amount of sensitive data being sent offshore that they're passing legislation restricting such activities. Some states require that you notify customers in writing if you're planning on sending their personal records outside the United States. How do you think your customers will react when they find out you're planning on sending their personal information offshore? You need to factor customer impact in when figuring out how much money you can save by sending work offshore.

Taking precautionary steps such as encrypting information, data scrubbing, using customer identification numbers instead of Social Security numbers and the like will position you well to deal with these types of issues. A little extra effort on the front end will not only reduce your risk exposure, but may also protect your company from new government restrictions as well.

The Law of Diminishing Returns

Annual wage increases for engineers in popular outsourcing countries such as India are outpacing those of their domestic counter-parts. Where in 2003/2004 you could utilize 8 Indian engineers for the price of 1 American engineer, that ratio has since dropped to 4 to 1. If you're engaging in a multi-year contract, make certain that you have strong contractual language in place to protect yourself from this trend.

Can off-shoring really save you money? The obvious answer is yes. However, it needs to be done responsibly. Think long and hard before giving engineers located half way around the world access to your company's internal network. Conversely, consider the risks involved in sending sensitive customer information offshore as well.

Philip Alexander is the author of the book [Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers](#) published by Greenwood Publishing