MONDAY, JUNE 26, 2006

Managing Subcontractors

Fourth-party outsourcing is sometimes authorized and sometimes a complete surprise! What do you need to know about placing controls on this practice or using it to your organization's best advantage?

Karen D. Schwartz

So you've decided to outsource some of your business processes for all the right reasons — you don't have the time or skills to handle the processes in-house; your employees need to spend more time on mission-critical issues; and you want to improve your organization's efficiency and reduce operating costs. You've done everything possible to ensure a productive outsourcing relationship, thoroughly examining your chosen service provider's business ethics and processes. You've signed the contract and you're ready to go.

You've done everything right, so you have nothing to worry about, right?

Not necessarily. Unless you have planned for the possibility that at least some of those outsourced processes will end up being handled by yet another contractor — one you didn't specifically scrutinize during the selection process — you simply can't be sure that your processes will run smoothly; your data and your customer's data will be safe and secure and that your business standards will be upheld.

The offloading of some of a customer's technology or business processes to a subcontractor happens more often than not — often with the customer's approval, but sometimes without the customer's awareness. Although fourth-party outsourcing or subcontracting, happens in the Business Process Outsourcing (BPO) arena, it tends to be more common with IT sourcing because processes like software development are easier to divide into distinct areas.

Signs of Subcontracting

There are several reasons why primary contractors may choose to subcontract some portion of a customer's work. In some cases, the deal is global and the outsourcer may not have a physical presence in some parts of the world, necessitating a series of subcontracts. In other cases, the outsourcer simply doesn't have the amount of skilled labor needed to meet the customer's requirements or is lacking in a key capability — typically hosting or security.

Subcontracting in itself is not inherently harmful; in fact, most of the time, it works quite well, and to the customer's benefit. But as with any outsourcing relationship, things can go awry for a variety of reasons — especially if they happen outside of the customer's control.

In addition to backlogs, lost money and time due to ineptitude and bad management practices, the subcontractor may have different security policies and procedures, and fail to follow your service provider's and your best practices.

"Their level of privacy, security, IP issues and performance could become real issues," says Atul Vashistha, CEO, neoIT. "Companies will start to see it either because they aren't getting the service levels they want or because violations will start occurring."

Skill level is another concern. Although you may have specified that your service provider's software developers must have attained Level 5 of Carnegie Mellon's Software Engineering Institute Capability Maturity Model (CMM-I), the subcontractor's employees may only have achieved CMM-I Level 2.

Companies may also be more subject to economic espionage, malicious destruction of software code and data piracy when subcontractors are involved. And if a prime contractor chooses to subcontract some of a customer's work to a provider in a different country from both that of the prime and the customer — countries whose laws and regulations have been clearly spelled out in the contract — these problems can be compounded ten-fold.

"You might end up moving the work of a company in a country with a democratic government to one with an authoritarian one or to a country with a different legal framework and police powers, with different levels of cooperation between law enforcement," explains Jody Westby, CEO, Global Cyber Risk, a legal advisory service.

Westby notes that the top three outsourcing countries — China, India and the Philippines — have no data-privacy laws, and the police in those countries deal with breaches in very different ways. "In India, for example, the police have overly broad powers in investigating cybercrime, and the United States has developed reasonable cooperation from the police in the Philippines due to the Melissa virus. In China, however, they basically do whatever they want," alleges Westby.

TALK BACK

Name: [   ] *   Email: [   ] *

Subject: [   ]

Comment: [   ] *

[Submit]   [Cancel]

GLOBAL SERVICES MICROSITE — Remote Infrastructure Management

NEWS | ARTICLES | EXPERTS' VIEWS | CASE STUDIES | RESOURCES | PODCASTS