



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?

by 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 Vashista, 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.

Risky Business

"Data-privacy issues can raise their ugly heads in unconventional but potentially harmful ways," agrees Mark Lutchen, Senior Partner, IT Effectiveness Practice, PricewaterhouseCoopers.

"Let's say you're outsourcing to India, but your outsourcer is at capacity and wants to outsource some of the work further to a company in the Philippines. The government and economic and political situation there aren't as stable, and the laws are different," explains Lutchen. "If you didn't stipulate that you want to have a server dedicated to you to protect your information, for example, [the subcontractor] might choose to house it with data from other customers. If the government launches an investigation into another company, they can demand the server, along with all of your customer's valuable information."

Problems like these are more likely to occur if the outsourcer chooses to subcontract some of a client's processes without approval — something that happens more often than people think, experts say — but, it can also happen even if the customer believes it has all of its ducks in a row.

"A lot of companies haven't thought about this and a lot of the master Service-level Agreements (SLA) have no restriction on moving the work to a subcontractor," says Westby. "If the vendor feels any concerns at all that the client will object, they may or may not tell them, and if they can transparently have the work done by a subcontractor, it is likely that they won't tell them."

"That certainly occurs, but reputed, established vendors would never pull a trick like that," says Ashok Syal, Managing Director, Sumpraxis, an outsourcer based in Delray Beach, Fla., with offices around that world that handles offshore transaction processing, engineering support and financial-support services.

"We never hide the fact that we're going to hire a subcontractor," says Syal. "The customer always knows the relationships. For the part of the work they do directly on a day-to-day basis, we even give them the names of the contact people there, and they work directly together. But the overall responsibility for making sure the project is successful and running smoothly is ours."

Once Bitten ...

When it comes to subcontractors, Bill Wood has been burned more than once — enough times to learn his lesson.

Wood, VP, Development, at Denver-based Ping Identity, a provider of identity solutions, has arranged many outsourcing relationships for his company over the years, and most have worked smoothly. Yet, when it comes to the issue of processes subcontracted by Ping Identity's hired outsourcer, Wood learned the hard way that it's not always in the company's best interest.

"When I look for an outsourcer, I'm looking for a company that has its own people, so I know they have the right training and loyalty to our company and everything else that's healthy to having a dedicated team," he says. "But when subcontractors are involved, sometimes the loyalties aren't as apparent. There have been times when we've ended up with subcontractors being represented as members of the team, but not trained in the tools and technologies the team should be bringing to the table."

Retention has been another problem. To illustrate his point, Wood points to a situation that occurred with an outsourcer in Mexico. Once the outsourcer subcontracted some of Ping Identity's processes, much of the workflow and goodwill Ping Identity and its outsourcer had worked so hard to create, became severely compromised. Many of the subcontractors' workers soon became restless and went in search of better offers. "They soon found more lucrative opportunities, leading to a very high attrition rate, which caused a problem for us," he recalls.

The lesson, Wood says, is that a primary outsourcer should only rarely parse out work — and with caution.

"It can work if you bring in a subcontractor for a specific reason, such as if they have a specific expertise that's required for a short period of time," he says. "That's very different from bringing in a subcontractor that spends months on the job."

To ensure no problems occur when subcontracting is allowed, Wood also recommends making sure the contract with the primary outsourcer specifies the number of subcontractors that can be part of the team in terms of a staff percentage.

—Karen D. Schwartz

The Right Way to Manage Subcontractors

Although there are myriad things that can go wrong with a fourth-party outsourcing arrangement, there are many steps a company can and should take before the original contract is signed with the primary service provider, to prevent many from occurring.

The first step is making sure your contract is ironclad, thorough, and, most importantly, gives you the right to approve or reject any proposed subcontractor in writing prior to any subcontractor being hired by the outsourcer.

"Our selection criteria for subcontractors is that we have to have had a working relationship with them for at least 15 years."

— Ashok Syal, Managing Director, Sumpraxis

"To avoid surprises, it's critical for the contract to specify that the service provider obtains prior written consent from the customer before any subcontracts are let," says William B. Bierce, Principal, Bierce & Kenerson PC, a law firm specializing in outsourcing representation. "In addition, it should say that all subcontractors have to follow the rules you set up for your outsourcer. Basically, everything applicable to the supplier has to flow down to the subcontractor. And you should include the right to audit how well the subcontractors are following the service provider's obligations."

Other clauses that should flow down from outsourcers to all subcontractors include conditions related to liability, non-disclosure, intellectual property, data privacy and termination.

Clients should also consider putting language into the agreement stipulating that although an outsourcer can select a supplier to deliver some subset of requirements, that subcontractor cannot do business with any of the client's competitors. They can also obligate their service providers to use specific subcontractors based on the client's specifications, notes Jeff Romano, a principal at The W Group, a consulting firm.

In addition to ensuring that your contract is ironclad, companies also should make a concerted and repeated effort to ensure that they know exactly what is going on at all contractor locations through periodic site visits and data audits.

"In setting up the governance, they should factor in what audits and reviews they need, if they need additional monthly conferences with the vendor as a checkpoint, and make sure to bring the subcontractor into that conversation," says Global Cyber Risk's Westby. "When you add in a subcontractor, everything expands and it's another layer you have to absorb."

Relationships Are Key

Trusting your primary outsourcer can also make a difference.

"Our selection criteria for subcontractors is that we have to have had a working relationship with them for at least 15 years," says Syal. "That way we know how they work and we can pretty much circumvent any problems related to lack of work ethic or other issues. In that time span, you know how much you can depend on that subcontractor."

Trust is crucial, but so is knowing when subcontracting makes sense and when it can cause more trouble than it's worth, says Dmitry Loschinin, CEO, Luxoft, a Moscow-based service provider.

"We start every outsourcing engagement by customizing our processes to satisfy the needs the client, and sometimes, that customization can be significant," says Loschinin. "When the customization is significant, or when the interaction between our team and the client's team is very intense, it doesn't tend to be a good situation for subcontracting," he says. "On the flip side, if the work relies primarily on standard processes and the work is neatly packaged into different parts with well-defined specifications, subcontracting can be a good option," he says.

But even if subcontracting turns out to be a good move, trust is still key. "It has to be a trusted partner you have confidence in. You have to check them out thoroughly," says Loschinin. "We always make sure our partner is well-trained and using the same tools we're

using, and that they are adhering to the same standards we have developed for our customer.”

“Because communication between client, provider and subcontractor is so critical to maintaining a good working relationship, provider-subcontractor relationships also tend to work best when both are located in the same geographical region — even the same office,” says Charles Spinosa, Group Director, Vision Consulting, an IT consulting firm.

“If the outsourcer and subcontractor are co-located, you can get a lot of seamlessness,” says Spinosa. “When you get people working close to the business, they form a team and have the same goals and intentions, and are less likely to go wrong. Just a few months ago we worked with a specialty outsourcer that wanted to subcontract to another party to develop a program. Shortly after the application was running in India, a big problem appeared. We were supposed to be told as soon as that happened, but we weren’t. We found out that the subcontractor had started writing incomprehensible notes to our traders trying to find out what was going on, and upon investigation, we found that the program couldn’t be compiled. That could have been avoided if everyone were working at the same location.”

“Communication and goodwill also can be fostered through simple events — events as commonplace as pizza parties and hosted meals,” says Spinosa. Even commendation letters go a long way toward creating a team atmosphere.

Companies should also take into account what type of processes are being outsourced, how regulated the industry is, and how critical the processes are when determining how much oversight to impose on both contractors and subcontractors. Anything related to intellectual property, data privacy and security should be tightly monitored, as should any processes governed by regulations such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA).

“If the risk and complexity is high, it makes sense to be more hands-on,” notes Vashistha. “If knowledge transfer is very important, for example, you would want to exercise more control over your subcontractors.”

But no matter how much oversight the customer chooses to have over subcontractors, managing the relationship truly is the responsibility of both the client and the outsourcer.

“I won’t pass on the responsibility of satisfying service-level agreements to my subcontractor. I would let him know that he’s responsible to me, and that he gets paid only when he satisfies our conditions,” says Syal. “If you drop the ball and let him work directly with the customer on the SLAs, slippage can happen. I’d say satisfy me first, and I’ll take care of the client.”

In fact, in subcontracting relationships that are working well, it’s not uncommon for the subcontractor, in some cases, to have ongoing direct contact with the client.

“Our contracts are with the primary outsourcer, but we have communication with the client,” explains Ranjan Sinha, Chairman, Summit HR Worldwide, a San Jose, Calif.-based offshore human resources outsourcing vendor that often acts as a subcontractor to primary vendors. “It’s a matter of the maturity of the relationship. Over a period of six to nine months, clients become more comfortable with the quality of service, and today we have numerous situations where the end client directly calls Summit. But it’s something that evolves over time, and rarely happens at the beginning of a relationship. It’s about the customer starting to trust us and the relationship.”

If All Else Fails.....

But what if, despite your best efforts, your organization still experiences problems as the result of a subcontractor arrangement?

Even if you have failed to put the necessary legal language into your outsourcing contract, experts say, any data or privacy breach caused by a subcontractor is considered a liability for your outsourcer, who hired the subcontractor — not your company.

That's little comfort, however, to a company whose reputation is compromised.

"If something goes wrong, everybody has a problem," says Bierce. "Although the contract generally puts the scope of loss on the shoulders of the prime contractor, the goodwill of the customer is damaged, and the relationship it has with its customers is damaged. Not only that, but it is legally liable in the country of loss to pay any fines that are due, and to make notifications required under various laws."

Although reputation is an issue, companies do have one recourse — mediation, and in extreme cases, termination of both the subcontractor and the prime contractor relationship for noncompliance.

Mediation, of course, is the first line of defense. By entering into mediation, the provider and client may be able to resolve differences amicably and salvage the relationship. But if all else fails, termination for noncompliance may be the only solution.

"If you can't remediate the problem through additional controls with the subvendor or additional lines of communication, you have to look at how you can terminate the contract and take the work back over or give it to another vendor," says Westby. "The priority is making sure you don't further jeopardize your operation."

Next

STEPS

- » Don't attempt any service provider relationship without competent legal input
- » Make sure your contract clearly states what type of subcontracting is acceptable, and that you must approve all potential subcontractors in writing
- » Monitor and audit all service providers on a periodic basis, including site visits
- » Communicate often and clearly with your primary outsourcer
- » Require that any approval is conditioned upon receiving appropriate information and documentation relating to the scope, nature and relationship of the prime to sub
- » Check the reputation of subcontractors
- » IT or business processes that include intellectual property or have the potential for data privacy and security risks and any process governed by government regulations
- » Be wary of subcontractors operating in different countries from your company and your primary outsourcer.