

How to survive your outsourcer's downfall

January 13, 2009

Ephraim Schwartz

http://weblog.infoworld.com/realitycheck/archives/2009/01/how_to_survive.html

Due diligence and up-front preventative investments are key to ensuring a smooth transition away from a scuttling -- or scandalized -- outsource provider

If the Satyam scandal out of Hyderabad, India, happened a couple of years ago, there might have been a lot of I-told-you-sos from folks who said using vendors thousands of miles away is risky business. But two years later, after the collapse of the largest financial institutions right here in our own backyard, followed by one of the biggest frauds -- the Madoff scandal -- ever, finger-pointing is not allowed.

[Therefore, I respectfully disagree with fellow InfoWorld columnist Martin Heller, who says Satyam fraud is a black eye for Indian outsourcing.]

Instead of focusing on one bad apple, the wiser choice is to look ahead and decide how best to protect your company no matter who your supplier is.

Primary due diligence: Vet and invest I spoke with a number of executives at outsourcing consultancies -- in other words, companies that don't do outsourcing rather they advise companies on how to do it -- in order to gain some insights into preventive business practices.

Before Steve Martin, partner at Pace Harmon, even spoke to me about what to do, he offered a caveat. While due diligence is key, even PricewaterhouseCoopers missed the hanky-panky at Satyam, and PwC was looking inside the books, he said. Caveat aside, Martin outlines primary and secondary due diligence that should be pursued.

First, you need to sit down with your prospective vendor at its physical location, the datacenter or the development center where the work will be done. Management should be interviewed, as should the project managers involved. Also, while you are there, look around. Make sure the vendor has a state-of-the-art infrastructure. Of course, as in the Satyam example, it wasn't the infrastructure that was faulty. Most companies will share only publicly available financial information, Martin says, but there are techniques to get behind that. For example, you should ask for the prior month's revenue statement.

"You can ask for a lot more financial information than is available publicly," Martin said, meaning, I believe, that if they want your business they will have no choice but to accept your prying eyes.

Of course, if you are going to assign any company tasks that have to do with mission-critical business processes or applications, you must perform a risk profile. In other words, before you go in, figure out what would happen if the vendor were to go down, whether through financial malfeasance, natural disaster, internal political turmoil, or terrorism.

Next, once a deal is struck, put the steps in place to facilitate porting an application or the infrastructure over to another entity easily. One way to do that is to make sure you are not dependent on a single individual or individuals at the outsourcer. Therefore, increase your dependence on documentation, data capture, and governance.

Industry-standard coding techniques and principles should govern your software development. How you develop code is indicative of how easily another software engineer can pick it up and reduce his or her learning curve.

Secondary due diligence: Background and backup plans

While Martin rightly points out that due diligence can go just so far and that even PricewaterhouseCoopers can be fooled, there is what some may call secondary due diligence that might have given Satyam's customer's pause. Again, we're not looking at Satyam in a retrospective sense but as an example of what can be avoided in the future.

Peter Harrison, CEO of Global Logic, another outsourcing consultancy, says there were signs of trouble with Satyam a number of years ago. Here's where a service provider that uses crawlers to aggregate external news sources and stories right off the Web or from media local to the prospective vendor can be of tremendous value. This is what is meant by secondary due diligence.

For example, I did a search on Satyam and came up with this story from 2006 about the World Bank, Satyam, and a case of bribery.

"When you talk to people on the street in India, you would have discovered that Satyam doesn't have a reputation for integrity," notes Harrison.

But as Harrison points out, this should not tarnish the reputation of all outsourcers: "Did WorldCom's imploding mean that companies should question using telecom carriers?"

Tom Pettibone, founder of Transition Partners, adds that "the commercial crawlers can spot things on the Web that join keywords like: 'offshore,' 'India,' 'sharp asset increase,' 'income discrepancies,' etc., but then somebody or something has to scan the article or blog for relevance."

Taking it a step further, Pettibone says you could use "quants" -- quantitative analysts who use highly specialized, home-grown analytics that can scan much more than just what's on the Web.

But there are plenty of things you can do yourself, says Pettibone. You should be sure that the vendor also has a business continuity plan. Ask to see that plan every six months if necessary. What happens if there is fire, flood, or fraud?

Also, have a secondary vendor with some of the same capabilities. Or better still, have two vendors share the workload. But this can be somewhat problematic, admits Pettibone, if the vendor is doing BPO, back-office processing, HR processing, or financial processing where it is more difficult to split the work.

Additionally, your company should have a small cadre of internal staff fully competent to take over the projects. Even if you are outsourcing a 200-person call center, you should have 10 people retained domestically who can re-establish that at another site.

There may also be direct financial repercussions to consider. If in fact a company is doing cash operations, receivables through a vendor that is about to disappear, you better know if your accounts are at risk.

If you find yourself in a dicey situation where a key vendor is going down, there are other considerations. Make sure you have the rights to hire those employees. If that is not possible, offer a "retention bonus" if necessary so that the vendor can retain key outsourced employees.

Returns on preventative investment

Say you expect to see a 40 percent savings from an outsourced project. Keeping local employees who can take the project over in the event of failure, or putting in place those retention bonuses up front, may chew up 20 percent of your projected savings, but can you really afford otherwise?

Even if nothing untoward happens -- the first time I've ever gotten to use that word in a sentence -- investing in the preventive measures outlined above will allow you to rebid contracts more easily.

As recent events have shown, it doesn't really matter if a service provider is down the street or halfway around the world; relying entirely on trust in business is not good for business.