

You've Outsourced The Operation, **BUT**

Have You Outsourced the Risk?

By Howard B. Whitmore

As growing numbers of U.S. and Canadian businesses look for ways to outsource business processes and operations to gain competitive advantages, they may fail to recognize that such activities can have a significant effect on an organization's risk profile. Managing potential exposures associated with outsourcing calls for a comprehensive approach, including a company-wide approach for identifying, measuring and mitigating such risk.

As businesses plan and implement outsourcing initiatives, there are several steps that can be taken to assess and manage these potential risks.

■ Vetting Potential Vendors

Analysis of potential outsourcing risks begins with taking a close look at a number of risk factors that can help a business establish some of the criteria it may use in selecting outsourced suppliers, vendors and distributors of its products or services. Assessing these types of issues can be challenging when evaluating potential

WHILE OUTSOURCING HAS BECOME AN IMPORTANT PART OF BUSINESS STRATEGY, IT PRESENTS YET ANOTHER AREA OF POTENTIAL RISK. AN INSURANCE EXPERT OUTLINES WHERE SUCH RISKS MAY BE LURKING.

vendors closer to home, say in North America, but the task can become more daunting in other parts of the world, where many firms are currently establishing outsourcing relationships.

When exploring such overseas opportunities, you may need to work with a consulting firm that can help vet vendors — including its principals — based on your own corporate guidelines, practices and policies.

When initiating a relationship with a vendor, it's key to align the vendor's priorities with your own business priorities and standards, and measure against these standards. For example, if a business is focused on reasonable costs and quality, it should look for suppliers that can meet its standards for availability, security, integration and distribution.

Similarly, if looking for rapid growth and developing new products and services quickly, then suppliers should be able to demonstrate that they

can scale quickly, adapt to change and maintain high production levels.

If the business is looking to expand and enter new markets, then suppliers must have the capability to deliver into those markets, and at the desired production or service levels. As such, they must be familiar with the culture, political landscape and environment.

Among the risk factors to consider for potential vendors:

Single points of failure within the value chain. For example, relying on a critical supplier with backup is risky. When possible, identify multiple suppliers.

Transition risk. Businesses need to understand how to avoid service interruptions when transitioning from one supplier to another, should this need occur.

Value risk. Companies must evaluate a supplier's ability to produce to its quality standards. This has become a huge issue as outsourcers in

many parts of the world are not able to produce product/s that meet a firm's quality standards.

Financial risk. Beyond assessing the financial stability of an outsourcing supplier or vendor, it's important to negotiate contract pricing properly. Understand how suppliers calculate price and what factors could cause it to fluctuate.

Innovation risk. Does the supplier understand your organization's future needs, and can it adapt and scale quickly enough to meet your demands?

Complexity risk. Can your multiple suppliers integrate effectively, or is there a potential significant risk of product and/or service breakdowns?

Hazard risk. Particularly in a new geography, the risk of loss from physical hazards and potential recovery issues must be evaluated — especially with respect to catastrophic exposures such as windstorm, flood and land movement.

Socio-economic and political risk. Know what exogenous risk factors could result from actions of foreign governments, as well as local social issues.

Businesses also need to determine whether potential vendors or suppliers meet their established standards for environmental, safety, labor and welfare practices. Consider the impact on your business if your vendor's business practices were not in line with your customer's expectations. Recall that in recent years, a number of clothing and apparel manufacturers and distributors have had to manage potential damage to their reputations when their vendors or suppliers were found to violate child labor laws and other labor practices.

■ Hazard Identification and Business Continuity

Once a vendor passes a company's "background check" and meets its other criteria, management still needs to consider potential business-impact issues. Among the priorities are to evaluate supply chain risks and adopt a business continuity plan. If such an analysis uncovers the lack of alternative supply paths, the

outsourced "solution" may not be viable. Even if there are alternative resource or supply options, it's still valuable to identify potential issues that could result in disruptions.

Established tools — such as catastrophe modeling earthquake and flood maps and other resources — may be non-existent or unreliable, for example, in some parts of Asia, where much outsourcing is taking place.

Coastal regions in Asia are prone to several typhoons each year, and key cities are subject to risk. In 1973, an earthquake in China with a magnitude greater than eight on the Richter scale resulted in the loss of 240,000 lives and the destruction of more than nine million buildings. Roughly 70 percent of China's land is subject to flooding, and many of the newly-industrialized areas are also flood-prone. Also, the availability of adequate supplies of potable water may be a risk issue, particularly in parts of China and India.

Such exposures may be analyzed with the assistance of a consultant or venture partner that is knowledgeable in local risk issues and has experts on the ground in these regions.

With a well-constructed business continuity plan in place and the hazards identified that could disrupt operations, management may choose to assess available risk finance or insurance options to provide needed capital in the event of a disruption.

■ Designing a "First-Party" Insurance Program

Thorough risk analysis and careful planning are critical elements of creating an effective risk-management plan. This information will make designing an appropriate insurance program more tailored and efficient. Negotiating and implementing insurance programs for international risks is generally a highly specialized activity.

Even if your vendor has insurance programs and adds your firm as an additional insured, you still have work to do. And, even after verification of the financial wherewithal of the vendor's insurer; confirmation that the compulsory programs are in

place; that the programs are placed with "admitted" (locally licensed) insurers, if required; and that contractual agreements are in place to protect your interests, many issues still need to be addressed.

It is important that your company's interests are protected and that your own insurance programs will indemnify you for your loss. Property insurance should be extended to cover the outsourced entity (watch for "territorial restrictions") for "contingent time element" coverages, which can pay for lost profits during an outage by an insured event. The programs may also be extended to provide extra expenses incurred by the insured firm to have these services provided by a backup/alternate source (or another party) while a vendor is out of commission — another reason why an effective business continuity plan is so important.

The time periods for which an insured company will get paid also need to be addressed. Is it enough to simply have the time it takes for your vendor to get back into business (standard), or do you want the additional time it may take your business to restore itself to its performance level prior to the loss, known as "extended period of indemnity?"

Even the time it takes to repair and replace damaged property may be subject to dispute, say, if technological obsolescence or upgrades for new code requirements become relevant. However, most of these potential issues can be addressed in a properly constructed insurance policy.

Today's cyber world presents unique exposure issues. For instance, the value of intellectual property, information on electronic media and whether the description of physical loss includes magnetic erasure are all issues that should be resolved with underwriters up front.

Considerations such as whether the insured perils include loss of power or other services that could create an interruption of services — even if there is no apparent "physical damage" — needs to be addressed. In the cyber world, definitions in an

insurance policy are critical.

■ Addressing Third-Party Liability Issues

Contracting with another party to provide or produce products or services, or components to provide services that will be perceived by customers as your service or product/s, presents a number of liability issues that may or may not be addressed effectively by a contract alone. These issues are further complicated when the outsourced operation is outside the U.S.

Will your vendor provide you with a “hold harmless” agreement? Even then, you must evaluate the practical aspects of its enforceability and the ability to collect under such an agreement. Additionally, a liability may be construed to be both yours and the vendor’s. Thus, it’s important to understand and agree on who will control the handling of liability claims — your company’s reputation could be at stake if customers or the general public are not treated in the same manner in which you treat them.

Also needed is clarity for handling injuries to employees that occur on a vendor’s premises. The definition of the employer-employee relationship may be different in countries outside the U.S., so businesses need to explore whether there may be circumstances in which the vendor’s employees could be considered your employees.

Another potentially challenging issue involves interaction between your employees and those of the vendor that might be culturally and/or legally acceptable in one jurisdiction, but unacceptable in the other — such as certain child-labor practices.

■ Esoteric Risk Issues

Most of the issues described above can

be addressed to some degree through the use of effective risk management and first- and third-party insurance programs. A number of other key exposures related to outsourcing need to be considered, evaluated, understood and addressed through the use of insurance.

Other “political risk” issues that businesses venturing outside North America may face include the potential of embargoes, the inability to get currency out of a country on a timely basis or the possibility of an industry being nationalized. Among the potentially insurable exposures for situations that result in the service contract being made inoperable or terminated are:

Political Violence/War: including war, civil war, rebellion, revolution, insurrection or civil commotion, that typically occur within a 25-mile radius of any premises of the service provider, and prevents its operations and causes it to default under the service contract;

Forced Divestiture: a law, order, decree, regulation or restriction by a local government requiring the vendor to permanently withdraw from terminate or make the service contract otherwise inoperable;

Selective Discrimination: including license cancellation by a foreign government that is selective and discriminatory, directed specifically against the insured company or a group of foreign-owned services providers in the relevant industry sector;

Government Act: (of the service provider’s country) that legally prevents the insured from fulfilling the service contract; and

Confiscation, Expropriation or Nationalization of property of the service provider.

In many areas, commercial insurance programs can be negotiated to address these exposures. These insur-

ance policies may typically indemnify the insured for the additional costs and expenses involved with having to relocate services such as:

■ Abandonment/relocation costs of moving any equipment, establishing and/or procuring necessary and comparable facilities in another country;

■ Extra contractual costs of working, including additional wage and/or operating costs following relocation, based on the same level of production and/or service as previously performed by the service provider for the agreed “period of indemnity;” and

■ Business interruption, although not typically included, can be negotiated to help the client recover lost profits from these actions for a pre-agreed period of time.

While there are a myriad of other potential risk issues associated with outsourcing, many can be addressed in part or full by various risk-management strategies. Among these are intellectual property issues, counterfeiting and IT security. And, in some cases, specialized insurance programs can address these risks.

Clearly, part of operating a business is taking risk, and risk/reward ratios are the subject of countless economic and business studies and strategies. Educated business leaders, armed with the proper information, can make informed, rational decisions that can leverage their assets for greater success.

Howard B. Whitmore (howard.whitmore@marsh.com) is Managing Director and Practice Leader for Marsh Inc.’s North America International practice, and is based in Richmond, Va. Marsh, the global risk and insurance services firm, services clients in more than 100 countries and is headquartered in New York.

- Outsourcing business processes and operations can have a significant effect on an organization’s risk profile.
- Managing potential exposures associated with outsourcing calls for a comprehensive approach, including a company-wide approach for identifying, measuring and mitigating such risks.

- When initiating a relationship with a vendor, it’s key to align the vendor’s priorities with a company’s own business priorities and standards.
- Among risk factors to consider for potential vendors are: value risk, financial risk, transition risk, innovation risk, hazard risk and socio-economic risk.

takeaways