4

Risks of Outsourcing

In the previous chapter, we examined reasons for outsourcing certain functions to service providers. In this chapter, we discuss factors, such as hidden costs, phantom benefits, and broken promises, that might be used to argue against such a decision. We shall return to the references that were used for the justification of outsourcing as they also suggest what risks or negative experiences customers had with outsourcing.

Loss of Control

The other side of the coin to handing over responsibility and blame to service providers is loss of control over outsourced operations. It is debatable whether a customer does—or indeed can—avoid some or all responsibility through engaging service providers.

The most common view of outsourcing appears to be that the concerns generated by giving up control override any sense of relief at not having the day-to-day operational responsibilities. This trend may result from perceptions regarding the different goals and attitudes of internal and external staff towards service, profits, and survival. Clearly much of the concern stems from customers' suspicions, which may be justified, that the outsourcer does not have the same level of commitment to meeting service requirements as an internal group. After all, as the argument goes, internal staff is more closely aligned to other insiders and subscribes to the goals, mission, and culture of the customer organization. However, this may be somewhat offset by greater formality, as embodied in explicit service level agreements (SLAs), which almost always exist in arms-length relationships between customers and providers, and are seldom seen between internal departments or divisions.

There are fundamental differences in motivation, goals, and attitude between internal staff and employees of outsourcers. However, these differences are not the same for all organizations and all situations. They can vary with the relative size of the customer and outsourcer, both to one another and, for the customer, to other customers. They will depend on the nature of the relationship—for example, whether internal staff members were transferred to the outsourcer's payroll or not.

The differences might also relate to the type of service being provided and the relative skills required of internal and external staff. The differences will surely vary over time as the personnel in both customer and provider organizations change, as the nature of the services changes, as competitive pressures build in the customer's world and for the outsourcer, and as the economic environment changes, within the industry, regionally, nationally and, increasingly, globally.

In the following sections, we will examine many of the factors that can negatively affect the posture and effectiveness of customer/outsourcer relationships. We will consider what can be done to mitigate the impact of these factors. We will also attempt to anticipate how these factors are changing over time and which of them will be exacerbated or moderated by general trends in the outsourcing business.

The principal risk drivers are the viability of the service provider, relative size of the customer, conflicts in service level agreements, legal liabilities, knowledge transfer, and hidden costs. We will look at these in detail in the following sections.

We show in Table 4.1 the relative objectives of each of these factors for the customer and the outsourcer respectively. The similarities or differences in objectives between each party impact greatly how each approaches the service relationship. Where they are similar, each party should be willing to compromise in order to optimize the relationship. Where they differ, we have the opportunity for contention, misperception, and damaging behavior.

Viability of Service Providers

Perhaps the worst nightmare of the customer of third-party services is the prospect that the provider will fail and leave customers in the lurch without access to critical services and systems. There have been a number of immediate and dramatic instances of failure of managed security service providers (MSSPs), which threatened the ability of customers to stay in business [1]. A number of outsourcers have reconstituted themselves and are looking to grow in their new form [2].

Table 4.1
Opposing and Common Objectives of Outsourcers and Customers

Factor—Objective	Customer (In-House)	Outsourcer (External)
Cost per unit of service—Opposing	Customer wants to obtain the most service for the least cost by: Carefully defining and controlling the services and related costs; Requesting proposals from a wide range of providers; Negotiating the most effective price (not necessarily the lowest price).	Outsourcer's goal is to maximize long-term profitability through: High price-to-cost ratio; Proposing flexibility in pricing rules to allow for additional revenue generation; Large volume of standard services; High customer retention; Economies of scale.
Quality of service—Somewhat opposing	Customer wants guaranteed aggressive service levels, adhering to prespecified metrics, with high costs (e.g., nonperformance payments) if the outsourcer does not meet the service levels. Customer wants compensation for business loss.	Outsourcer prefers looser or nonexistent service-level requirements with minimal give-back in the event of not meeting any specified service levels. Provider wants to be responsible only for subscription fee.
Control—Opposing	There are two customer views: Customer retains control by having staff and capabilities in-house that can assert control. Customer hands over control and responsibility to the service provider and does not maintain in-house capability. Here, the reliance is on the service contract to ensure that third party performs and enforces requirements.	Outsourcer prefers having greater control since, among other benefits, it makes it harder for customer to terminate services and perform the services in-house or at a competitor's facility.
Viability of service provider—Similar	Customer wants to retain a service provider that is likely to be around for the duration of the contracted services, and extensions if needed or wanted. Customer does not want to have to react to a sudden change in ownership of the service provider (including none) that might lead to the discontinuation of critical services.	Outsourcer wants to be perceived as a long-term player and not an organization presenting the specter of failure. An ability to demonstrate long-term viability attracts more customers and is self-fulfilling since the additional business supports the outsourcer's remaining viable.

Table 4.1 (continued)

Factor—Objective	Customer (In-House)	Outsourcer (External)
Viability of service provider—Similar	Customer needs to be careful not to necessarily retain the lowest bidder since that firm could be in trouble and be desperately seeking additional business just to stay afloat and may not be successful.	
Viability of customer—Similar	A good cost-effective outsourcing deal can, in many cases, increase a customer's profitability and make it more competitive, therefore it is more likely to survive and compete effectively.	Outsourcer should concentrate on customers with a good record and realistic business plans and who appear to be outsourcing for the right reasons, rather than as a survival tactic. The rise and fall of the dot-coms represents an example of an industry whose demise threatened, and in some cases took out, otherwise healthy service providers and vendors. Bottom line: The customer needs to be able to pay its bills.
Setup—Similar	From the customer perspective, it should be relatively painless to establish the service relationship and its concomitant systems and services.	From the service provider perspective, it should be relatively efficient and fast in establishing the service relationship and its concomitant systems and services. This will accelerate the start of the income stream from the customer.
Discontinuance—Opposing	From the customer perspective, it should be relatively painless to sever the service relationship and its concomitant systems and services.	From the service provider perspective, it should be a relatively difficult and lengthy process, but inexpensive (to the provider) for the customer to extricate itself from the service relationship and its concomitant systems and services. This will extend the income stream from the customer as much as possible. The anticipation of the process being difficult also might discourage present customers from closing down their relationship. Another ploy is to engage the customer in as many of the outsourcer's services as possible, which will make extrication even more difficult.

Table 4.1 (continued)

Factor—Objective	Customer (In-House)	Outsourcer (External)
Operation—Somewhat similar	The services and systems provided by the outsourcer should integrate well and easily with other customer operations. This might require, in some cases, considerable customization of the services and systems.	The service provider also wants the systems and services to integrate well with existing customer systems and services, which the service provider is not able to replace oris not interested in doing so. However, the outsourcer's preference is for its customers to use the "plain vanilla" systems and services, with a minimum of customization. The more the systems and services are tailored to the meet the customer's requirements, the more difficult the support and the more resources required to maintain the specialized system and services.
Scalability—Similar	From the customer's perspective, the outsourcer's systems, networks, and services should be able to be easily scaled to meet increases in business volumes and changes in business mix. All this ties in with the cost model that customers seek, namely, elimination of fixed cost and pricing based on variability of activity volume (e.g., number of transactions).	For the outsourcer, it is advantageous for the systems, networks and services being offered to be scalable so that additional customers and business volumes can be accommodated easily and quickly. It is preferable for the incremental costs of the additional services and systems to be very low, but the market should be such that the outsourcer can charge substantially higher prices.
Complexity—Opposing	The systems and services might be complex "under the covers" but should be simple to use.	The systems and operations should be easy to maintain and change, but there should be a high cost of entry for customers and/or competitors trying to in-source and/or compete, respectively.
Ease of use—Similar	The systems and services should be intuitive and simple, requiring a minimum of training and fewer calls to the help desk.	The systems and services should be intuitive and simple, requiring a minimum of customer and technical support.

In order to reduce the risk of such failures, it is important that customers follow a clear, structured approach to minimize the chance of being subjected to such a failure or to reduce the impact if such a failure does occur. Before entering into a service-provider arrangement, the prospective purchaser of the services should perform a complete and detailed due diligence process [3, 4]. Additionally, the agreement between the customer and outsourcer should anticipate the potential failure of the service provider and include provisions for such an event. These provisions should include a set of contingency plans allowing the customer organization to avail itself of alternative facilities and resources or to take over those resources of the outsourcer that have been applied to the customer's particular service. The operational contingency plans need to be exercised and rehearsed on a regular basis to ensure that they will work.

At the time of failure, a predetermined response plan should be put into effect to protect the outsourcer's customers from the negative aspects of such a failure, which might include effecting negotiations with other vendors.

Reasons for Abandoning Service

There are many reasons why a company might go out of the service-provider business. Some are due to internal factors, such as poor management, inadequate funding, and employee misdeeds. Others relate to external factors, such as industry trends, downturns in the general economy, and mergers and acquisitions.

One of the most insidious causes for failure is damage to reputation. This can be real or perceived. But either way, the results can be the same—abandonment by existing customers, reticence of new customers to sign up, loss of key staff, and more.

A major factor can be broad awareness of customer dissatisfaction if it is made known through disparaging articles in the press, badmouthing among industry members, or other forms of communication. And it is not just the larger customers who can be harmful. Dissatisfaction expressed by smaller customers can be just as damaging to a service provider as complaints from larger customers, particularly if the smaller customers band together and give voice to their unhappiness through the press.

Mergers and Acquisitions

Mergers and acquisitions can affect customers in two ways. The most obvious is the acquisition of the service provider. The question then arises as to whether the acquiring company wishes to continue providing the specific service or prefers to close down or sell that particular operation.

In another scenario, a company might acquire an existing customer and then the latter or its owner may transfer to a competing service provider, perhaps the one that is already being used by the acquiring company. Another reason for leaving might be that the acquiring company already provides the service in-house and wants to internalize the outsourced services.

Such changes can threaten the existence of a service provider and represents some risk to the customer.

Relative Size of Customer

Generally, a particular customer is one of many serviced by the outsourcer and most likely accounts for only a small percentage of the total workload of the service provider.[1] Sometimes smaller customers feel that they are second-class citizens in the mind of the outsourcer, relative to larger customers from which most revenues are generated. Bigger customers may get special price breaks, customized services, and dedicated support staff—features that may not be available to the medium-sized and smaller customers at all, or may be unbundled and charged for at a high premium. In the event of general problems, larger customers may have their concerns addressed first, with small customers waiting until support staff is freed up from dealing with the larger customers.

Sometimes a large customer will successfully assert its dominance in order to obtain preferential treatment. However, if that customer is in contention for service with another even larger customer, it may itself have problems getting the desired attention. Also, in such a competitive battle for service, the customer may gain priority by making the most noise and escalating the issue to upper management at the provider. Smaller companies can avail themselves of this technique also and move up the priority ladder based on aggressive requests or special relationships with senior staff. Sometimes a customer might appeal to former employees who have transferred to the provider, thereby getting privileged access to decision-makers. Competition between customers for the provider's attention is a common situation. And it takes a top-flight service provider to be evenhanded in its treatment of customers.

In some situations, larger clients provide the economies of scale that make costs lower for everyone, including smaller customers. The latter should understand that the large clients might in fact be subsidizing them. On the other

[1] If a service provider has many customers (for instance, more than 50), it is to be expected that the 80-20 rule, or similar, will apply, whereby 80% of business belongs to 20% of the customers. Sometimes the percentage is more skewed, with a handful of large customers and hundreds of relatively small organizations.

hand, the larger clients are often able to negotiate sweeter deals with the outsourcer just because of their size and volume of business. With their unequal risk profiles and different motivations, outsourcers and their customers approach the outsourcing relationship in different ways, as depicted in Table 4.1.

Quality of Service

One of the main reasons to outsource is the expectation of receiving better service from the outsourcer than from internal staff. This expectation is often based on the knowledge that there will be an explicit SLA in place, which can be enforced by the customer and which might bear remedies against the outsourcer for nonperformance. While companies are increasingly establishing SLAs for internal providers, they are often harder to enforce since everyone is a member of the family.

If an outsourcer loses a customer because of poor service, it is much less excusable. Of course, the perception of poor service could be misguided, or service expectations may not have been realistic in the first place. However, SLAs between customer and provider generally specify what constitutes acceptable service and what does not. Therefore, a base set of metrics exists against which to measure performance. The SLA is discussed in greater detail in Chapter 6.

There is a strong argument that the measures in an SLA may not adequately depict the perceived service. In an article by Jiang et al., quality measures are categorized into tangibles, reliability, responsiveness, assurance, and empathy items [5]. Some items are typical of those included in a SLA, whereas others are not. The quality measures include the following categories.

Tangibles

In *tangibles:*

- The service provider has up-to-date hardware and software.
- Physical facilities are visually appealing.
- Employees are well dressed and neat in appearance.
- Appearance of the physical facilities of the information systems unit is in keeping with the kind of services provided.

Reliability

In *reliability:*

- When outsourcer promises to do something by a certain time, it does so.
- The outsourcer provides services at the times promised.
- The customer insists on error-free records, and the outsourcer agrees.
- When users have a problem, the outsourcer's information systems units show sincere interest in solving it.
- The outsourcer's information systems units are dependable.

Responsiveness

In *responsiveness:*

- The outsourcer tells customers' users exactly when services will be performed.
- The outsourcer's employees give prompt service to users.
- The outsourcer's employees are always willing to help users.
- The outsourcer's employees are never too busy to respond to users' requests.

Assurance

In *assurance:*

- Behavior of the outsourcer's employees instills confidence in users.
- Users feel safe in their transactions with the outsourcer's information systems units' employees.
- The outsourcer's employees are consistently courteous with users.
- The outsourcer's employees have the knowledge to do their jobs well.

Empathy

In *empathy:*

- The outsourcer's operational hours are convenient for all their users.
- The outsourcer gives users individual attention.
- The outsourcer's technical units have employees who give users personal attention.
- The outsourcer has the users' best interests at heart.
- The outsourcer understands the specific needs of users.

The only item that can be related specifically to security or, more precisely, integrity of the service is the reference to error-free records in the reliability category. Many of the measures do not typically appear in SLAs, but are often key in evaluation and selection processes. Interestingly, security is only alluded to in one item in the assurance category in regard to feeling safe.

However, it is noticeable that there are no specific security metrics. The measurement of security characteristics is still in its infancy. There are no absolute standards and probably never will be, since the environment is continually changing and the needs of security are changing in response.

Since absolute security is not achievable, it follows that measures are likely to be relative. Some current standards are set and the actual operation can be measured against them. TruSecure Corporation, in defining their measures for certifying security posture uses the term "essential practices." This underscores the fact that the term "best practices" is not an accurate depiction due to the frequent occurrence of new threats and the discovery of previously unknown vulnerabilities. The latter could result from a detailed examination of the application or system code, a random event, or a directed attack by a computer worm or virus.

Nevertheless, the aspects of security that are characterized by system and network availability and system and data integrity are more measurable. Availability, in particular, can be expressed in specific percentage terms. However, even for availability, issues exist as to what are appropriate measures, since providers and users may have differing views, as described in my articles on the user's view of availability and reliability [6, 7].

Brandon and Siegelstein list occurrences, which make a system unavailable, in their book on contract negotiation [8].These occurrences are:

- The system fails to operate.
- The system fails to operate in accordance with formal specifications.
- The system operates inconsistently or erratically.
- The system is in the process of being maintained or repaired.
- A hardware or software component of the system is inoperative, which renders the entire system useless for user purposes.
- The system is not operated because there is potential danger from operation of the system to operators, employees, or customers.
- There is a defect in software supplied by the manufacturer.

These factors all affect the availability of a system to a customer's users, even though some factors may be controllable by the service provider and others are not. An important goal of the service arrangement is to establish that the outages due to controllable factors will be minimized. This is usually more difficult to do when the resources reside at, and/or are managed by, a third party.

Definitions

In order to assist in your determining what availability and reliability mean in this context, here are some definitions of applicable terms:

> The *reliability* of a system is the probability that, when operating under given stated environmental conditions, the system will perform its intended functions adequately for a specified interval of time.
>
> The *availability* of a system is the probability that the system is operating satisfactorily at any point in time, excluding scheduled idle time.
>
> *Intrinsic availability* is the probability that a system is operating in a satisfactory manner, when used under given conditions, at any point in time, excluding idle time and downtime other than active repair time.
>
> *Operational readiness* is the probability that a system is either operating or can operate satisfactorily when it is used under stated conditions.

The probability that a system is operating is a function of the mean time between failures (MTBF) and the mean time to repair (MTTR).

More detail in this area is available in the cited references and in standard engineering texts on system reliability. It is well worth learning some of these details. The availability component of quality of service is often the most contentious aspect since there is generally room for a range of interpretations and misinterpretations as to whether a service level is being met.

The Issue of Trust

It has become very important to ensure that third parties who have access to personal and confidential information are protecting that information from inappropriate disclosure and from misuse. In particular, customer organizations are increasingly being held responsible for securing and protecting customers' information. As mentioned earlier, a burgeoning body of laws and regulations holds boards of directors and senior management directly responsible for any breaches that disclose nonpublic personal information (NPPI), in particular to those who might exploit it for fraudulent endeavors.

The issue of trust has recently taken center stage in the health and financial services industries in the United States, the United Kingdom, Europe, and other countries around the world. A slew of laws and regulations require the protection of end customers' NPPI from unauthorized access and from misuse by those with or without approved authorization. In these and other sectors, there is also concern in regard to unauthorized and unintended disclosure of corporate and government confidential or proprietary information, as well as intellectual property.

Even prior to the extensive privacy and security legislation and regulation of recent times, which have focused on the protection of customers' identifying information,[2] there were very valid and forceful reasons to limit access to information when transmitted and stored electronically.

Such protection is not only altruistic but is often related to preventing competitors from gaining access to customer lists for fear that they would steal customers. In financial services, requirements keep information known to investment bankers away from traders, brokers, and other individuals who might attempt to use such insider information improperly. Such requirements also extend to third-party service providers who have access to the same information.

It is one level of effort to protect confidential, personal, and otherwise sensitive information within the confines of a single institution. Imagine how much more difficult it is to protect such information when it is obtained and processed by service providers, which may not be bound by the same laws and regulations as their clients. Of all the aspects of outsourcing, information protection is often the most critical, especially, as we have noted, in financial and health services, as well as government sectors, such as law enforcement and defense, where secrecy is paramount.

As will be discussed later, it is difficult and often costly to satisfy executive management, boards of directors, and regulators that sufficient care has been taken to safeguard the privacy of individuals' data. Safeguards include ensuring protection of information against unauthorized access or false manipulation during creation, transmission, storage, and retrieval operations involving third parties.

Another complication arises when different laws and regulations govern both the customer organization and the third party, particularly when located in different jurisdictions such as different states in the United States or different countries Accordingly, heavily regulated financial firms make extraordinary efforts to ensure that their service providers comply on their behalf and on

[2] The U.S. Congress, along with other legislative bodies around the world, continues to express serious concerns over the proliferation of identity theft and the use of personal information against the interests of the owner of that information, namely, the private citizen. As mentioned previously, members of Congress, at a Subcommittee Hearing on cyber security at which I testified, clearly indicated that they had concerns about identity theft. In fact, I got the distinct impression that the issue of identity theft superceded cyber security in their minds.

behalf of their retail customers with relevant laws and regulations *as they apply to the customer organization.*

A U.S. financial firm, for example, is required by their regulatory bodies to retain and have quick access to certain documents for periods of several years. Therefore, in order to be acceptable to the financial institution and its regulators, service providers must arrange to offer and maintain such storage and access capabilities in their handling of those documents, in paper, electronic, or other form, in a manner consistent with the financial institution's regulatiory requirements. In such cases, it is not enough to have a statement or response from the service provider to the effect that the documents are stored and available appropriately. It is necessary for the financial firm to review the policies, standards, procedures, and other documentation relating to such data creation, transmission, storage, and disposal by the service provider *and by any subcontractors of the service provider.*

It is also good practice to test whether the outsourcer's stated policy and procedures are enforced and implemented. Either the customer organization or the service provider may hire third-party auditors or security assessment consultants to perform security and control assessments. Such specialty assessment firms are likely to do a more orderly, structured, and complete evaluation than an in-house staff might achieve, because they perform so many more assessments over a period of time than would an in-house group.[3]

With respect to support functions, an internal support group, whether a user help desk or technical support group, is usually dedicated to assisting internal personnel or direct customers of the firm. On the other hand, service providers' support groups will likely have many more customers vying for their attention. This raises concerns that an outsourcer's support may not be of as high a quality or as responsive as that of the firm itself, when the support function is internal. However, there is a strong trend towards outsourcing customer and technical support to third parties domestically and offshore, with mixed success.[4] Since, in many cases, support does not need to be colocated with the

[3] Nevertheless, these third-party security assessments are not guarantees of absolute security, and should not be taken as such. Security assessment is not an exact science and, to a considerable degree, depends upon the expertise and experience of the testers. I recently had the experience where a second evaluation of the same application unearthed a vulnerability that had been missed by a prior assessment by a highly reputable firm. Also, the assessment is good only at particular point in time and should be redone whenever a major change in architecture or functionality occurs. It is recommended that security tests for highly critical systems be done with regularity and by different consulting firms. It is also very useful to have an internal group able to perform such assessments as an additional check, if such a group can be cost-justified.

[4] In one highly publicized example, Dell Computer actually pulled back a help desk operation from India to a domestic U.S. facility because corporate customers were complaining that the quality of service was inadequate.

main service facilities, such support is frequently put in remote places where there might be a shortage of jobs and wages are lower. This also applies in regions where the cost of labor is less, as in near-shore and offshore locations.

Much of the evaluation of support is subjective and qualitative. The support area is rife with measurement problems. Service metrics include the number of requests handled per unit of time and in total, time to respond, and time to resolve the issue. Such measures usually are more relevant to the operation of the support group than to the customers. However, customers are certainly affected by the service levels, in terms of how long it takes to get through on the telephone (numerous rings, busy signal, on hold, or diverted through a complex automated response system), how knowledgeable the support person is, and how quickly and accurately the problem is resolved.

Sometimes, what appears to be a high service level, in terms of increased number of calls handled per hour, is not necessarily a good thing. A large on-line brokerage firm found that following the introduction of a telephone response system the number of calls increased dramatically, in part because the system was easy to use and individuals took advantage of the faster system to ask more questions. From the firm's perspective, there was little added value to the incremental calls since they did not generate additional revenues.

Customers often have concerns that the service provider will not meet required service standards. These concerns can usually be mitigated through contractual language. More likely, the service given is often in direct response to the service demanded. Customer organizations need to be willing to assert their contractual rights in getting better service, possibly through escalation or the threat of escalation to outsourcers' senior management. If that is not effective, the terms in the agreement need to be enforced, which might involve payments to the customer organization or reduced charges. If the matter is still not resolved, it may become necessary to take legal action and prosecute the terms of the contract, although this is clearly the least desirable action, since it will lead to strained relationships between customer and service provider and additional costs for both parties.

Performance of Applications and Services

Support is only one aspect of service. Another is the performance of the actual services, be they IT applications, operational services, or something else.

Again, SLAs should be designed to account for levels of performance of the contracted services. Here, too, metrics can assist. Measures of capacity, throughput, response time, and availability—particularly availability—are frequently used in SLAs to monitor performance.

However, since the outsourcer has profitability in mind, its goal is to provide service within the agreed-upon limits at minimum cost. Sometimes, if the penalties for not meeting the performance criteria are not onerous, the outsourcer might find that it is cheaper to fail on the performance criteria than to add capacity and redundancy to meet or beat the criteria. It is important, therefore, to ensure that any payments back to the customer are sufficient to motivate the service provider to meet the service requirements.

It is also important for the availability criteria to be applied to significant times of day, days of the week, and so forth. A failure during a period of peak volume will have much greater impact than one that occurs during off-hours.

To maintain a proper balance between capacity and cost, it is necessary to establish the criteria up front and allow for changing requirements. Otherwise, performance needs of customers may not be met over time as the customer's volume and/or the volumes of other customers increase.

Lack of Expertise

It can often be difficult to find third parties with a proven team of experts who are experienced and knowledgeable in a particular industry being serviced or in specific computer applications, programming languages, or system platforms. Customers should beware of bait-and-switch tactics. Vendors should provide lists of their staff along with their résumés as part of the outsourcer's proposal, and customers must insist that specific individuals be assigned to the project or service. Additionally, the customer should retain the right to approve any substitutes. Another safety measure is to ensure that the applications or activities outsourced can, if necessary, be insourced or contracted out to a different provider.

Hidden and Uncertain Costs

There are two main reasons why certain costs may be overlooked or hidden from the due diligence evaluation of service providers.

First, some costs are very difficult or practically impossible to quantify. Intangible costs might relate to such aspects as perceived quality of service.

Other costs are easier to define, but the probability of their occurrence is very uncertain. Such is the case with outsourcer viability. Reasonably good estimates of the cost impact of failure of a service provider can be made, but the probability that the outsourcer will fail is uncertain, particularly at the time of the evaluation. In fact, if outsourcers were known to be having financial difficulties at the time of the evaluation, they should not have been included in the short list of finalists. However, even though an outsourcer is in financial distress, it might continue to provide services. Additional funding (from a venture capitalist, for instance) could save the outsourcer or the provider might be acquired by another company, perhaps a competitor.

In the case of acquisition, services to specific customer companies may or may not be continued, at the choice of either the provider or the customer. Outsourcers are sometimes acquired by a competitor of one or more of their customers, in which case the latter might decide to terminate the service at the earliest opportunity. Some astute customers include statements in their contract with the outsourcer to the effect that either party can end the relationship, without termination payments, upon acquisition by a third party of either customer or provider.

The range of possible outcomes adds to the uncertainty. I have often heard, in response to negative financial news about a service provider, that "someone will buy the company and keep the service going." History has shown that such a resolution is by no means certain. Some form of risk analysis is called for in these circumstances in order to estimate the probabilities of each outcome and to project the corresponding costs.

In risk analysis, however, some costs might be hidden or excluded altogether, either unintentionally or through the analyst's ignorance or inexperience. More insidiously, an analyst may intentionally exclude costs to favor one decision, such as selecting one provider versus another, choosing insourcing over outsourcing, or staying in a particular business or not. Whatever the predisposition of the analyst might be, these intentional oversights or unintentional errors have to be dealt with differently, but they all must be confronted. There are well-publicized instances of major business decisions having been made due to errors or omissions in the calculations, as mentioned earlier.

While many domestic and offshore outsourcing decisions are based on known, tangible costs and benefits (such as cost savings), others rely on less tangible costs and fuzzy benefits for their conclusions. Furthermore, actual events have a major influence on the analyst's expectations of the likelihood and magnitude of future events. For example, the successful terrorist attacks of September 11, 2001, revised everyone's expectations of the frequency, scope, and impact of devastating terrorist attacks. Legislators and regulators have responded with conservative backup and disaster recovery requirements, particularly in critical sectors such as financial services.

The greatly increased expectations of the probability and magnitude of terrorist attacks, the wars in Afghanistan and Iraq, the threats posed by North Korea and other nations, and the potential for the global spread of diseases (such as SARS) have raised management concerns about offshore outsourcing. As a result, management has focused on contingency planning, business continuity, and disaster recovery for offshore facilities.

In response to these concerns, management in many domestic organizations using offshore service providers launched investigations of outsourcers' contingency plans in the event of a war or other disruptions. Management wanted to know whether domestic facilities and capabilities could take over in the event that offshore facilities were no longer available. Of course, similar requirements apply to domestic outsourcing, where the chance of war may be less but the expectation of terrorism is high. Suddenly, the security and continuity risk equations for critical functions such as technical support and applications development changed and are now considered subject to the whims of terrorists. The huge increase in expected losses resulting from recent terrorism, wars, and health epidemics, in addition to the vagaries of the economy, has created a much greater willingness to expend funds to mitigate such risks with increased investments in security, business continuity, and disaster recovery.

Such potential losses were not anticipated when originally evaluating many outsourcing proposals—how could they have been? In hindsight, the analysis was in error. Had such terrible events been factored in, the decision to adopt a particular outsourcing arrangement might have actually been reversed in some cases to avoid the newly recognized risks or the costs of mitigating them. While some analysts favor a high reserve to allow for extremely uncertain events, such as acts of war or terrorism (often termed "force majeur"), it was far more common not to allow for such highly unlikely scenarios prior to September 11 than subsequently. Of course, one might argue that the telecommunications industry did not, as a whole, consider the potential bursting of the dot-com bubble, which in many ways was far more devastating financially to many organizations and individuals than the various terrorist acts.

Table 4.2, illustrates the differences between situations in which there is an understatement of costs and/or overstatement of benefits and situations in which the expectation of something happening was explicitly included or not.

In Table 4.2, if the analyst misses something that should have been anticipated, that is a sign of incompetence. If the analyst misses something that someone expert in the area would likely miss also, he or she is not to blame, because

Table 4.2
Predictable and Unpredictable Oversights

	Likely to Be Anticipated	**Unlikely to Be Predicted**
Oversight (Accidental)	Less usual—reason for concernabout the ability and/or intentions of the analyst	Usual situation
Hidden (Intentional)	Fraudulent	Unprofessional (given the benefit of the doubt)

events that could not have been guessed in advance occur frequently. If the analysis intentionally omits something that should be generally known by someone familiar with the area, it is a fraudulent act and, if provable, needs to be dealt with severely. If an analyst omits something that is difficult to know about or it is hard to estimate its impact, the analyst is being professionally dishonest if he or she chooses not to disclose that such an event could happen and would affect the analysis if it did indeed happen.

Limited Customization and Enhancements

Going into an outsourcing arrangement, it might appear that the systems and/or services meet most if not all of customer's requirements without the need for future enhancements. However, situations change over time, both for the outsourcer and the customer organization, and need to be renegotiated if they were not in the original contract. Most changes of this nature are readily accommodated.

On the other hand, a customer's business might change due to external market forces or new laws and regulations, and the demands on their outsourcers change accordingly. To the extent that the demands of a customer and the provisions in the outsourcing agreement diverge, there are implicit as well as explicit costs to the customer related to satisfying the discrepancies, even to the extent of having to transfer to a different service provider or to an in-house operation.

Knowledge Transfer

The more functions and roles that are outsourced, the less likely is it that the internal staff can support those functions should they be moved back in-house. In order for an organization to maintain its best bargaining position and to retain critical internal staff, the latter must be kept up-to-date by means of training programs and/or via the transfer of knowledge from the outsourcer to the customer. Rotation of customer staff through the service provider on a prespecified schedule might be feasible. Of course, the outsourcer will probably not be enthusiastic or supportive of such an exercise, since it is in their interest to keep customers dependent on them.[5]

[5] I once was involved in an effort to move a computer system in-house from a "facilities manager," as host service providers were once called. We were able to achieve a great deal on the operational side—taking over the entire computer job production-control system. In this way, the internal expertise was built up.

The cost of not maintaining a knowledgeable cadre of internal staff can be considerable in the long run. The impact can include loss of negotiating power in terms of costs and services, difficulty in moving to another service provider or in-house, and the danger of being totally dependent on a third party whose strategic direction might not match that of the customer. For the most part, these costs are difficult to measure and are usually excluded from the evaluation of the outsourcing relationship, but they are real costs.

Shared Environments

A major concern, especially among firms in highly regulated industries such as financial and health services, is one customer gaining access to information about another customer. Beyond the risk of having a competitor get access to proprietary information, there would be the strong possibility that a firm is not in compliance with laws and regulations. Such a case is not purely a business or reputation risk, but puts senior management and boards of directors in jeopardy if found to be negligent about ensuring that customer information is protected.

With a function operating totally in-house, there is little likelihood that other companies can access information—unless, of course, industrial espionage or information warfare occurs. However, if these same systems and data are moved into a shared environment, such as an outsourcing arrangement, this new, very serious risk appears. How should this risk be mitigated? There are several possible approaches, such as vulnerability analysis and tests and enterprise security evaluations and certification. But, it is important to note that the outsourcer's status might change.[6] The customer needs to be notified in a timely fashion.

Legal and Regulatory Matters

Increasingly, legislators and regulators are looking at the issue of the security of customer data. The risks related to not protecting customer data adequately apply not only to the individuals tasked with managing those information assets but also to senior management and the board of directors. The real strength of these regulations lies in their application whether or not the information is in the hands of the organization to which it was originally entrusted. That is to say, a firm's management is just as culpable if the disclosure took place from inside a

[6] I know of a situation where an ASP was considering moving its own computer facilities from in-house to a hosted service. It was only by chance that the customer got to know about it, much to their chagrin.

third party not under the former management's direct control. This has led to a frenzy of due diligence, particularly by the larger U.S. banks, which are subject to the Gramm-Leach-Bliley Act and the consequent regulations by the Federal Reserve Board, Securities and Exchange Commission, and other agencies.

Certainly, from a basic perspective, the cost of the newly required and intensive due diligence efforts and the risks associated with not meeting the regulatory requirements need to be included in the evaluation of all outsourcing arrangements, particularly where customer NPPI is transferred to and from the outsourcer.

The long-term effect of these requirements is likely to be a reduction in the number of service providers serving highly regulated markets and a consolidation into a relatively few major players. These stringent requirements also suggest that some form of globally recognized certification standards needs to be developed and the means of attaining them established. While certifications might increase initial costs, they tend to lower the longer-term aggregate costs because certification standards must be met periodically, perhaps annually, versus being continually subject to verification.

Summary and Conclusion

When all the risks of outsourcing are considered, one wonders how anyone ever makes the decision to use a third party. However, there is plenty of evidence that these deals are done frequently and are often satisfactory from both buyer's and seller's perspectives.

The purpose of this chapter is to make the reader aware of the risks and pitfalls involved in the analysis and evaluation of third-party service providers, particularly from the security aspect. Once aware, the evaluator should be able to develop a satisfactory analysis and service arrangement and, consequently, arrive at a decision that is justified through the consideration of all factors, and not the neglect of an unpleasant few. For the latter will surely raise their ugly heads and negatively affect the area of outsourcing. Better to be prepared in advance for the appearance of hidden costs and the possible occurrence of unlikely events than to be taken by surprise.

References

[1] Berinato, S., "Security Outsourcing: Exposed!" *CIO Magazine*, August 1, 2001, http://www.cio.com.

[2] Wright, R., "The Hosts with the Most: Three Hosting Companies Revamp Their Channel Strategies. What's in It for VARs?" *VAR Business*, June 2, 2003, http://www.varbusiness.com.

[3] Allen, J., et al., *Outsourcing Managed Security Services*, Carnegie Mellon University, Pittsburgh, PA: Software Engineering Institute, January 2003, available at http://www.fedcirc.com.

[4] "BITS Framework: Managing Technology Risk for Information Technology (IT) Service Providers," *Banking Industry Technology Secretariat,* Washington, D.C., November 2003, http://www.bitsinfo.org.

[5] Jiang, J. J., et al., "Closing the User and Provider Service Quality Gap," *Communications of the ACM*, February 2003, Vol. 46, No. 2, pp. 72–76.

[6] Axelrod, C. W., "The User's View of Computer System Availability," *Journal of Capacity Management*, Vol. 2, No. 4, 1985.

[7] Axelrod, C. W., "The User's View of Computer System Reliability," *Journal of Capacity Management*, Vol. 2, No. 1, 1983.

[8] Brandon, D. H., and S. Siegelstein, *Data Processing Contracts: Structure, Contents, and Negotiation*, New York: Van Nostrand Reinhold Company, 1976.