Payoff

Outsourcing is the process of contracting a third-party information systems vendor to perform all or part of a company's information technology functions. It has become synonymous with systems operations, systems management and facilities management. INPUT, an industry consultancy focused on outsourcing trends, predicts an 18% compounded annual growth rate in the U.S. outsourcing market over the next five years. It can therefore be expected that regardless of their industry focus, many information-dependent organizations will evaluate outsourcing as an alternative to internal management of information systems.

Introduction

Outsourcing can encompass a variety of information technology functions. Any function can be outsourced: systems operations, Transaction Processing, application development and maintenance, network management, and microcomputer integration and maintenance. The decision to outsource depends on a combination of logistical, organizational, and financial considerations.

Historically, outsourcing has been more common in mainframe environments. But as a result of downsizing, companies are increasingly inclined to outsource desktop services, including LAN administration and maintenance.

Why Outsource?

The primary motive for considering outsourcing is cost reduction. Long-term outsourcing contracts convert variable costs to fixed costs, and make technology spending more predictable. The tax advantage comes from the ability to deduct the expense of outsourcing fees from current year earnings as opposed to depreciating an internal data processing department's hardware assets over time. Outsourcing agreements can yield capital for cash-strapped organizations if the outsourcer purchases the client's hardware assets. In addition, companies who outsource enjoy cash flow improvements resulting from the transfer of software licenses and personnel to the outsourcer, and the release of obligation from a facility lease and the associated physical plant maintenance costs of a data center.

Outsourcing providers guarantee service and system availability. Their data center facilities are outfitted with redundantly designed systems to avert power and cooling failures and to detect water leakage, smoke, or excessive heat—anything that will adversely affect system continuity. Furthermore, the operations procedures of outsourcing providers—which might include advanced system and communications monitoring tools and specialized professional training—are designed to ensure uninterrupted processing and network availability. Leading-edge data center facilities are costly to operate; the expense can rarely be justified without the economies of scale derived from a shared environment.

In an outsourcing relationship, software and hardware upgrades become the concern of the outsourcer rather than a distraction to senior management. The client no longer deals with day-to-day information system details and can focus instead on business planning. Executives are freed from having to spend hours evaluating technology directions, technology funding plans, and the resulting vendor proposals. The outsourcer should be

---

charged with maintaining service levels for current needs and providing timely and cost-efficient technology solutions in support of the proposed strategic direction.

Hiring and retaining highly trained technology professionals is often cited as an additional incentive to outsource. The core business focus of outsourcing providers is technology. Their personnel are highly informed about emerging technologies and their implementation within specific industries. This level of knowledge is shared by their security professionals as well.

Types of Outsourcing Arrangements

In an outsourcing arrangement, everything is negotiable. Some of the most common arrangements are:

- Specialty Transaction Processing only (e.g., payroll and credit card processing including data communications from the data center to the client site).

- Systems operations (e.g., operations and maintenance of mainframe hardware and systems software) including data communications from the data center to the client site.

- Systems operations and applications development (e.g., operations and maintenance of mainframe hardware and systems software combined with application programming and maintenance) including data communications from the data center to the client site.

- LAN hardware and or software administration in a microcomputer environment which may or may not be connected to a mainframe by means of a network.

- Any of the preceding combinations plus distributed mini-and microcomputer systems. This is the most complex environment, with mainframes, mini-, and microcomputers all connected via a network.

The type of outsourcing arrangement selected directly affects the type of information security issues and concerns that will be encountered. Because communications networks are a key component in all of the previously mentioned arrangements, security and access issues are particularly pertinent.

Given space limitations, this article focuses primarily on the second and third options given—that is, systems operations and systems operations and applications development. Some microcomputer and LAN issues are discussed when appropriate because PCs and LANs can compromise mainframe security no matter how well the mainframe itself is secured.

Security Strengths and Weaknesses of Outsourcing Arrangements

There are several advantages to outsourcing arrangements. The outsourcer's information security staff can often provide valuable insight, in a confidential manner, about how other companies handle the same types of security problems.

The outsourcing company's information security administrators and systems programmers specializing in information security can be a valuable asset to the client organization. For example, the outsourcing provider may be able to help the client reengineer access rules to tighten security or to react to regulatory changes. The outsourcer may provide valuable information when your applications programmers perform a data base migration or an update that involves internal application security, and may be able to
provide product recommendations, thereby saving the client's staff from a lengthy evaluation process.

Aside from the benefits derived from the outsourcer's data center experience and internal resources, clients stand to gain from the overall information security environment. Because outsourcing providers have strict contractual obligations to their clients and must maintain their reputation in the marketplace, their control procedures are usually well documented and enforced.

On the minus side, a shared environment with multiple clients poses more risks than the contained environment of an internal data center. In multiple client sites, LANs, Wide Area Network, dial-up access for multiple clients increases the points of exposure: the risk of third-party employees having access to data; the risk of more than one client sharing Direct Access Storage Device or spool, the risks inherent to data transmissions; the risks of sharing a network; and in some cases the risk of sharing Central Processing Unit under one operating system or under separate logical partitions. In addition, other clients may have gateways to the mainframe from LANs and other distributed systems. A small exposure can grow several orders of magnitude larger in an outsourcing environment because of the sharing of resources with the outsourcer's other clients.

These risks are addressed by the outsourcer's physical and logical security procedures. The greatest risk comes from poor up-front planning and poor communications between outsourcer and client.

**Dividing Up Responsibilities**

In the new environment, the company's information security becomes a cooperative effort between the client company and the outsourcer. Whereas the outsourcer is the custodian of the data, the client is still the owner.

Planning is of the essence. Great attention must be given to determining which parts of the information security function should be performed by the outsourcing company and which should be handled by the client. Because the client company still owns its data, it should reserve some of its staff to monitor the security work handled by the outsourcer. Therefore, it is not advisable to transfer the entire security staff to the outsourcing company. Although the outsourcer's staff will most likely handle the routine functions of maintaining a secure system, the client's staff must monitor internal compliance with the outsourcer's security policies and procedures as well as internal information security.

The following paragraphs discuss responsibilities for performing specific security functions.

**Installation and Maintenance of the Information Security Software**

Information security software is an integral part of the operating system. In an environment where the mainframe and its system software are being controlled by the outsourcing company, it would be wise to also have the outsourcer's staff support the information security software. It can be installed and maintained either by the group that installs the operating system or by the outsourcer's information security group.

**Access Control and Security Administration**

Responsibility for such administration depends on whether the information security function is centralized or decentralized. In a centralized environment, one group of people is primarily responsible for setting up log-on IDs, writing access rules, and ensuring compliance with information security policies and procedures. If information security is currently administered in this manner, it should probably be kept that way.

However, because outsourcers are ultimately responsible for the integrity of the information security data bases, they will probably prefer to have their own security staff actually add and delete log-on IDs and write the access rules on the client's behalf. The
client’s group may be limited to making updates to existing log-on IDs (e.g., resetting passwords and suspending terminated employees). Requests for new log-on IDs or for access rules would be approved by the client’s security staff first, then passed to the outsourcer’s information security staff for processing. In this manner the outsourcer’s information security staff could ensure that the client is not inadvertently creating security exposures.

In a decentralized information security environment, security administrators may be assigned locally to each of the client’s departments or divisions. These local administrators set up log-on IDs and write access rules for their area only; they are not able to make changes to log-on IDs or access rules belonging to another department or division.

Centralized control results in a more consistent implementation of information security and its associated policies and procedures. If administering information security centrally is not a viable option for an organization, it is critical that the information security staff monitor the work done by local security administrators to ensure that the integrated security procedures of the client and the outsourcer are implemented consistently throughout the company.

Violation Report Review and Investigation
The outsourcing company should provide the client with the necessary data for violation reports. However, the review and investigation of these violations are probably best handled by the client's own information security staff because they are more likely to know which data is critical. In addition, because the client's security staff is most familiar with internal personnel and operations, they can move more quickly to follow-up on security violations. The outsourcer's information security staff should be available as needed if additional investigation is required to resolve a particular problem.

Relationship of the Outsourcer's Information Security Staff with the Company's Users and Customers
A company that prides itself on its personal relationship with customers probably wants to keep contact with the outsourcer's staff minimal and only at the company's request. The company may also act as a liaison between the outsourcer and customers if contact is required to resolve a problem.

It may also be desirable to handle internal users' contacts with the outsourcer's information security staff in the same manner. Many problems and questions concerning information security are specific to company policies and procedures; these can be better explained by the company's own staff. If the outsourcer is to handle users' information security problems and questions, guidelines should clearly delineate what the outsourcer's staff should handle, whose authorization is required to address routine information security problems, and what types of issues should be referred to the company's own information security staff. A good outsourcing company should insist on clear guidelines so neither the company's internal staff nor its customers feel like they’re getting the runaround when trying to resolve security problems.

Responsibility for Information Security Policies and Procedures
The outsourcing company has its own internal information security policies and procedures, as does the client company. Incompatible policies can create problems. Therefore, it is important to check for conflicts in the company's and the outsourcer's information security methodology as early in the process as possible. It is easier to resolve problems early rather than later, after everything is locked in. The outsourcer can provide help in writing or revising company policies and procedures.

Responsibility for Security Awareness Training
Although the company is ultimately responsible for ensuring that its employees receive the proper training, the actual training sessions can easily be turned over to the outsourcing
company. The company should ensure that the outsourcer and company are in agreement over class curriculum.

**Outsourcing Security Issues**

This section of the article addresses several security issues that are specific to the outsourcing environment.

**Sharing Computer Resources with Other Clients of the Outsourcer**

One of the major functions of the outsourcer's information security group is to ensure that its clients do not compromise each other's processing environment either intentionally or unintentionally. With some outsourcers, several companies may share the outsourcer's computer resources. For example, processing may be run on the same Central Processing Unit; this might be done under separate logical partitions or under the same operating system. If computers are to be shared, the client company should verify that other clients cannot access the company's applications.

With shared Direct Access Storage Device and shared tape devices, the outsourcer's other clients may be able to access the company's data, even if processing is not shared. Security software should be implemented to prevent such exposures.

It is very likely that client companies will be sharing a network. There are various ways to implement network security, including several network security products that recently have become available that interface with the mainframe's information security software. The outsourcer's network security methods and software tools should be identified and evaluated. The Service Level Agreement should specify the network security controls desired by the client.

**Assurance That the Company is not Billed for Another Client's Use of Resources**

A charge-back software product can solve this problem. In addition, information security software should be used to ensure that only authorized log-on IDs use cost centers belonging to the company.

**Information Security Audit Rights of the Client Company**

As noted earlier, the outsourcer should give the client's information security staff the ability to review (and in some cases, update) its log-on IDs and access rules. The outsourcer should also give audit authority for those same log-on IDs and access rules to the client's auditors. It would, however, be counterproductive for the outsourcer to allow all of its clients' auditors to do a full system audit whenever they wish. Instead, the outsourcer should regularly provide clients with the results from full systems audits performed by a mutually agreeable third party.

**Outsourcer's Access to Client's Data**

To ensure the availability of the client's data, some of the outsourcer's staff need to access the company's data. The challenge is to determine what the outsourcer needs to know and what is the appropriate level of authority for data access.

The outsourcer's internal policies and procedures should be consulted to answer these questions. Is the outsourcer staff required to sign confidentiality agreements? Does the outsourcer have stringent access controls? Is its staff bonded? Are policies and procedures enforced and disciplinary measures clearly stated? Which types of individuals on the outsourcer's staff have powerful privileges and why?

If the company plans to outsource its applications programming to a systems management provider or to a third party, it should ensure that there is a methodology to create test data as opposed to copying current production data into a test file.
application programmers should be prevented from updating production data. There should be an emergency procedure in place to fix production problems in a controlled manner and provide an audit trail of what was done and why.

**Determining Ownership of Data and Programs**

The client owns its business data; the outsourcer is a mere custodian of that data. But what about the data governing the outsourcing relationship? Who owns the billing information? The performance data? The client should determine which data actually belongs to the company and which data requiring the company's access belongs to the outsourcer. This distinction is important when it comes to writing access rules, because the data owner determines who is allowed access to that data. The distinction between these should be clearly spelled out in the service-level agreements.

If applications programming is outsourced, information security should have a prominent place in the development cycle. A test methodology should be in place so that copies of production data are not copied into test files. Appropriate change control procedures should also be in place.

Even ownership of policies and procedures can become an issue. If the outsourcer writes policies and procedures for the client but owns the copyright, the client company cannot change the policies and procedures without approval from the outsourcer. The contract should transfer intellectual property rights and copyrights to the client so the client can update procedures in the future and take them at the end of the outsourcing arrangement.

**Data Retention, Destruction, and Backup**

Responsibility for data backup should be clearly defined. This decision should take into account the most efficient and cost-effective method of backup.

Outsourcing providers may have automated backup tools that can make the efficiency question easy to answer. As data management becomes more and more automated, it becomes increasingly important for the guidelines regarding data retention, destruction, and backup to be completely documented.

The outsourcer's chargeback rates for data storage are based on the requirements for availability and performance of data sets. Space on a high performance disk drive is substantially more expensive than that on tape. The rates directly affect management's decisions regarding how and when data is backed up and archived and to what type of storage device.

Service-level agreements regarding data management should clearly spell out exactly what is required in terms of retention, destruction, backup, and performance. In addition, it should be ensured that the data is protected adequately until destroyed in accordance with the guidelines in the service-level agreements.

**Security and General Management Issues**

There are some areas for which the information security staff is not usually directly responsible but which must be considered. Several of these issues are discussed in the following paragraphs.

**Physical Security**

It should be verified that the outsourcer has adequate physical security to meet the client company's needs.

**Change Control**

The outsourcer should have implemented an adequate change control methodology. The client company should always be informed of any hardware or software changes that could
affect it. These types of changes could involve anything from installing a new Central Processing Unit to upgrading the security software. In addition, the client's staff should be given the opportunity to test these changes before they go into production and provide feedback to the outsourcer regarding the test.

Disaster Recovery
The outsourcer should have an adequate disaster recovery plan and a contract with a reputable hot-site vendor that has a configuration that will meet the client company's needs. The hot site should also have a backup plan, and it should have physical security at least comparable to what the outsourcer has at its regular site. It should also be verified that the security software is fully functional when processing at the hot site. The client company's staff should be involved in testing the disaster recovery plan on a regular basis, and the plan should be updated as needs change.

Regulatory Requirements
The outsourcer should be able to handle any special regulatory requirements the client company may have. For example, a bank has to deal with bank regulatory agencies; an investment firm with SEC regulations. The outsourcing company should be made aware of any special requirements and its ability to meet the relevant industry's regulatory demands in a timely fashion verified.

Service-Level Agreements
Service-level agreements are critical in the outsourcing business. The client company and the outsourcer must know exactly, in writing, what to expect from each other. The quality of the service-level agreements directly affect the quality of the relationship between the client company and the outsourcer.

The outsourcer will probably go out of its way to ensure that the client is satisfied with the agreements. Do not assume anything—if its important, get it in writing. Outsourcing contracts generally are in effect for three to ten years. A lot can happen during that period—people are reassigned to other projects, are promoted, leave the company, or simply forget. Nonetheless, an outsourcer should allow for reasonable interpretation of the service-level agreements during the life of the contract.

The information security service-level agreement should specify the services expected from the outsourcer's information security staff and what functions will be retained by the client's staff. For example, if the outsourcer is setting up log-on IDs and access rules for the client company, expected turnaround times and accuracy rates should be indicated.

The service-level agreement should also specify how emergencies will be handled. Whose authorization is required to fix specific types of problems? Which problems are to be handled by the client's staff and which by the outsourcer's staff? Will there be 24-hour-a-day coverage from the outsourcer's staff or is coverage during normal business hours sufficient?

The agreement should also indicate how special requests will be handled. This includes customizing information security software and implementing interfaces between information security software and applications. Will there be additional cost associated with these special requests? And, what kind of turnaround time is expected on these types of changes?

Preventing Conflicts
It should be verified that other departments of the client company that deal directly with the outsourcer also have written service-level agreements and that these agreements do not conflict with those written for information security. For example, consider the
consequences of conflicting procedures when a production job abnormally terminates in the middle of the night as a result of a security violation. The information security service-level agreement may state that before the outsourcer's staff writes the access rule, they must secure authorization from the client's information security staff to ensure that data is not compromised by inappropriate change control procedures. Concurrently, computer operations may have a service-level agreement written with another department in the client company that states that abnormal terminations will be fixed within two hours, regardless of cause or resolution. If the client information security staff could not be reached within the stated period of time, the resolution window would be missed, which would probably result in conflict and finger-pointing the next morning.

The service-level agreements should indicate courses of action that can be taken if the agreements are not met. Often, service-level agreements include bonuses for service delivery above stated standards and penalties for substandard service. Only very serious service-level agreement breaches allow the contract to be terminated.

It should be remembered that service-level agreements are a two-way street. If the client company does not fulfill its end of the service-level agreements, the results can be equally devastating. The client should understand the liability associated with information security breaches by either party, including the limitation of damages. There are legal implications if either company fails to fulfill its obligations; this should be adequately covered in the contract.

In November 1991, new sentencing guidelines from the United States Sentencing Commission took effect. If a company or its employees is involved in criminal activity (which can include breach of information security), the company is now exposed to monetary penalties substantial enough to push the company into bankruptcy and to court-ordered supervision of its future business activities. To protect against such action, both the client and the outsourcer must have effective information security policies and procedures so as to prove in court that both have an effective compliance program in place. Any fines will be substantially lower if it can be shown that an effective program is in place.

**Conclusion**

Because companies outsource their data processing for a variety of reasons or, at some point, at least investigate the possibility of outsourcing, the need for writing thorough service-level agreements cannot be stressed strongly enough. It is important that everyone involved, both at the client company and at the outsourcer, knows exactly who is responsible for each function in order to prevent misunderstandings. (Exhibit 1 summarizes the responsibilities of the outsourcer and the client.) It is also important to make information security an issue at the beginning (i.e., during the outsourcing selection process) to ensure a successful outcome.

**Outsource and Client Responsibilities**
Outsourcer
----------
--Installs and maintains data security software.
--Writes and maintains data center data security policies and procedures.
--Quality ensures client's log-on ID structure and access rules.
--Sets up log-on IDs and access rules according to agreed-on specifications.
--Provides data for violation reports.
--Supports client liaison to internal users and customers on as needed.
--Supports client training through technology transfer; may deliver training on contract basis.
--Upholds service-level agreements and enforces policies and procedures to protect all clients.
--Implements regulatory compliance procedures in a timely fashion.

Client
-----
--Defines business needs and identifies data security issues.
--Writes and maintains internal data security policies and procedures.
--Defines structure for log-on IDs and access rules.
--Approves log-on IDs and access rules as implemented.
--Updates log-on IDs.
--Investigates and resolves violation reports.
--Acts as liaison between outsourcer and internal users and customers.
--Arranges or provides data security training for internal users.
--Adheres to stated policies and procedures and ensures internal compliance.
--Provides outsourcer with regulatory requirements.

Author Biographies

Marie Alner

Marie Alner has more than 15 years of information security experience in the financial services industry. Since 1991, she has been an information security consultant for Integrated Systems Technologies, Inc., the information systems outsourcing subsidiary of First Data Corp. Alner is currently the president of the New England ACF2 user's group and is a member of the ISSA and CSI.