WHITE PAPER

Mitigate BPO Security Issues

OSF Global Services

INTRODUCTION

Business Process Outsourcing (BPO) is a common practice these days: from front office to back office, HR to accounting, offshore to near shore.

However, benefits of reduced cost aside, improved efficiency and increased expertise of outsourcing – you need to provide outsourcers with access to some of your most sensitive corporate data assets. So, along with the benefits of BPO comes an **increased risk to data**.

If you cannot protect your data, you put your business at risk. However, if you constrain the use of data too much, you can paralyze the outsourcing effort – and your business.

So how do you **align your outsourcing effort with business goals** while protecting the data? This white paper aims to give you some practical tips on what to ask and to expect in an outsourcing relationship, in terms of security.

TABLE OF CONTENTS

Specific information security challenges in outsourcing

There is a series of security challenges related to outsourcing, which is why the implementation of security controls calls for a quite close collaboration between the customer and the service provider. The actual amount of collaboration necessary and the resulting challenges depend on the **scope of the security controls that you outsource**:

- Service providers can handle **virus scanning** and **vulnerability management** with little interaction with the customer;
- **Business continuity planning**, **incident management**, and **review/audit of the service provider** are security controls that require considerable interaction between the outsourcing partners.

Additionally, there is a series of outsourcing-specific information security challenges. Most of them arise from a key principle concerning security in outsourcing: **liability for information security cannot be outsourced**. This principle is part of many regulations, and it imposes at least two fundamental requirements with regard to the implementation of information security in outsourcing:

- The customer must be able to determine the type and level of security controls that are operated by the application service provider (ASP).
- The customer must be given the possibility to audit and review the implementation of security controls by the ASP.

The challenges are…

Problems appear also because **the customer's infrastructure is embedded in the service provider's infrastructure**. For instance, an outsourcing client's mail server is accessed and operated from the service provider's management consoles. Thus, an outsourcing client has to make sure that the service provider's measures to secure its own infrastructure are adequate for providing the level and quality of security services the outsourcing client desires.

This is a list various outsourcing-specific **sources of information security threats**:

- Shared infrastructure for multiple clients;

- Differences in the legal systems of the outsourcing client's and the service provider's countries;
- Subcontracting to additional service providers with inadequate security controls by the service provider;
- Contracting parts of the same business process to two different service providers;
- Bankruptcy of the service provider;
- Acquisition of the service provider by another company with different priorities;
- Employees who reveal confidential information that belongs to the customer.

Key security facts

Low labor costs and an abundance of workers have translated into big returns for businesses that look offshore for technical support, telemarketing, payroll accounting, or credit card processing. While this is a very good means to cut costs, it can also pose great threats, leading to losses in credibility, and, in the end, money.

In 2007, companies including Bank of America, ChoicePoint, Citibank, and Time Warner experienced the **loss of customer information** or reported **intrusions into their data banks**. In one security breach in 2007, three former employees of MphasiS, a company providing outsourcing services, were arrested for stealing more than $350,000 from four customers of Citibank. The workers were accused of acquiring passwords and transferring money from customers' bank accounts into their own. Concerned over security at foreign call centers, other U.S. companies that engage in BPO ask themselves: **Is it worth the risk?**

According to John C. McCarthy, vice president for research at Forrester, some outsourcing providers forgo background checks of employees and even help applicants dress up their resumes. McCarthy surveyed 91 U.S.- based IT companies and found that, of those that were actively investigating or using offshore call centers and customer-service providers, nearly two-thirds of them were cutting back on their contracts or taking a closer look at the vendors' security practices.

Security is everywhere in the outsourcing lifecycle

You must keep security in mind during the whole outsourcing process, because each phase has its own specific characteristics, challenges, and possible solutions. This is a list of the most important steps to

take to make sure you manage security challenges for your best interest in the complete outsourcing cycle:

- **Preparing to outsource.** BPO sets security expectations, and each outsourcing model has different risks – that is why new control structures will be required. You should consider the implications of future changes (of the outsourcing relationship, or of the ASP itself) and identity critical and sensitive assets in terms of data security. Two logical actions should follow updating your security policies and standards, and reviewing systems against standards in order to decide how to manage compliance gaps.

- **Due diligence.** Always check the security of suppliers: customer references and certificates are only a start. Even if there is no substitute for a professional, independent review, at least prepare a set of carefully selected questions – small & medium enterprises should seek external advice. You must check the skills, experience, and qualifications of the service provider's staff. In this respect, aim for best value, rather than lowest cost in labor.

- **Developing and negotiating the contract.** The contract specifies the services required, how they will be delivered and by whom. It should also define the processes to manage change, rectify non- compliant deliverables, and resolve disputes. Negotiations should aim to define standards and processes that are acceptable to both parties – a solid service level agreement (SLA) will protect you from possible breaches from the ASP.

- **Ensuring confidentiality and privacy of data.** In your relationship with the ASP, the two parties must reinforce policies by education, vigilance and audit. Maintaining a map of where sensitive data is stored and processed helps pinpoint where the process needs additional controls. Use data leakage prevention technology to manage data flows.

- **Building flexibility for future change.** Post- contract changes attract high charges, so agree to processes for periodic review of standards and controls in advance. Legal and regulatory requirements must be binding across all current and future sites and sub-contracts.

- **Managing the contract.** Essential governance processes will need to be adapted to operate across the partnership. Here are some **tips**: set codes of practice to define and agree on expectations; have a proactive strategy in relationship management; aim for a win-win partnership with shared incentives; and build relationships with the right people at the right level.

TIPS

Have a realistic security policy that includes data classification and that distinguishes common from sensitive data, as well as how you should handle each type of data.

Make sure the service provider you use has strict security policies too, starting with the hiring process. This rule applies to all types of vendors, but especially to offshore companies.

Make sure that the vendor you chose is willing to abide by your privacy and intellectual property policies since a misunderstanding can be costly.

Quick checklist for choosing an ASP

When you evaluate an ASP for its security maturity there are some critical points that you should assess primarily, to define the degree in which that ASP has relevant background:

- Network protection
- Incident response
- Host hardening
- Security policies and plans
- Security patching
- Application development
- Encryption requirements
- Password policies and procedures
- Privacy
- Employee background checks
- Disaster recovery
- The ability to respond to security incidents

These areas are similar to the requirements of ISO 17799; however, the ISO framework does not specify particular answers against which an ASP may be measured.

You need to be very specific, so that the ASPs are able to understand and respond appropriately to your queries. By being specific, the ASP has a clearer understanding of your metrics on every point – and whether their procedures are close to your metrics.

Specific requirements for ASP's

Information security should be on every supplier's due diligence list as you review suppliers. However, it is difficult to find a clear metric for security. For example, one cannot determine the number of attacks that were discouraged or the number of unhappy employees who decided not to attack because of strong information security. Thus, you should consider the following **indicators of good security in an ASP**:

- A written and realistic security policy;
- A management with a visible commitment to security;
- Evidence that the supplier has assessed security risks, understood legal requirements, and implemented steps to address the security risks;
- The supplier's operational team, when interviewed, shows a good understanding of security issues and demonstrates satisfactorily how the supplier deals with those issues;
- The supplier has adopted a well-accepted security standard, such as ISO/IEC 17799 Code of Practice for Information Security Management, the U.S. Department of Commerce's NIST Special Publication 800 Series, and the ISO/IEC TR 13355 Guidelines for Management of IT Security;
- The ASP has a disaster recovery arrangement in place, backs up data regularly, requires a keycard to access key facilities, protects all databases with passwords, and makes background checks a condition of hiring employees.

Potential customers should also inquire as to whether the supplier performs services under the legal controls that affect the customer. If the prospective supplier is not already complying with the regulations affecting the customer, the latter should seek assurances that the supplier is willing and able to comply.

What you should have in a solid outsourcing contract

Outsourcing agreements should include provisions requiring information security. For example, the supplier should agree to:

- Keep confidential all information provided by the customer, on behalf of the customer, or as a result of performing services for the customer;
- Abide by all relevant privacy laws including those listed in the agreement;
- Allow security audits on the supplier's systems, including hiring an "ethical hacking" firm to test the strength of the supplier's firewalls;
- Protect all information whether or not confidential with appropriate physical and logical controls. For example, access to customer data should require user IDs, passwords, and a need-to-know authorization process. The supplier should agree to provide the names of all persons with such access upon request;
- Revoke access for any user upon a security breach or customer's request;
- Use reasonable efforts, including employment of industry-standard virus protection software, to avoid viruses, worms, back-doors, trap doors, time bombs, and other malicious software;
- Provide a copy of all customer data in the supplier's possession or under its control, in a reasonable format, upon customer's request;
- Never grant any subcontractor access to the supplier's data unless the supplier has approved the subcontractor and the subcontract includes all of the security provisions of the outsourcing agreement;
- Report all security breaches or incidents to the customer;
- Have, maintain and follow an acceptable business recovery plan (including disaster recovery, data backup, alternate power, and similar topics).

These are merely a few examples of what a solid outsourcing contract should contain, and different provisions will be appropriate in different types of outsourcing transactions.

Tactical steps in ensuring security

Today there are numerous new technologies designed to address the issue of security in outsourcing. These new technologies are helping enterprises with outsourcing projects underway to improve data risk mitigation techniques. Likewise, enterprises considering BPO in the future are building data security into their outsourcing strategies. **The first step** in securing outsourced critical data **is data discovery**. Knowing where specific data reside and who is accessing them will provide the basis for an effective monitoring program. Data discovery locates and monitors unstructured data assets (data in file servers) as well as structured data (data in databases) and legacy applications as well as open systems. Ideally, you should be able to identify specific types of data in these applications such as Social Security numbers or credit card numbers.

Once you have established a benchmark for data location and access, you can create policies for monitoring, alerting, and reporting. The main goal of monitoring is to provide detailed information on how, from where, when, and by whom data is being accessed, and then to have the ability to analyze that data against policies related to compliance regulations, data protection/data breach detection and corporate data governance programs. Policies for compliance are among the easiest to create. Some auditing/monitoring solutions come with pre-defined policies covering the major regulations such as SOX and PCI.

The second step is compliance. Despite the fact that these regulations look complicated, the auditing requirements are very straightforward. You can write actions – such as alerting and pre-scheduled reporting - into policies to automate the monitoring process even further.

Creating policies for data theft is another critical tactical step you must take. There are definite signatures for theft – such as highly sensitive data accessed, data accessed at odd times, unusually large downloads, or, more importantly, certain combinations of these – that can easily be captured in policies. However, detecting data theft requires more than just the right policies; it requires sophisticated analytics that can look at specific behavioral characteristics against history and then factor this data into the determination of data risk.

Determining the right solution for your organization depends on a number of factors including:

- How many data servers you need to monitor
- How much traffic flies over your network
- What type of output you require from the system — types of reports, workflow features, alerts, etc.

Conclusion

A certain amount of risk is a natural part of doing business. However, when it comes to data, many companies must accept more risk than they might otherwise be comfortable with because the bottom line benefits of outsourcing outweigh the risks.

Once you assess and then find the right ASP, the outsourcing relationship must be handled very carefully, in order to protect your data. **Real trust** is one key word in this process, together with **solid legal provisions** and **modern technology**.