Addressing the Risks of Outsourcing

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they simply don't have the resources, experience, or capabilities to do perform the tasks themselves.

> According to a 2005 IDC report, the global market for outsourced IT services hit $84.6 billion in 2004. IDC expects:
>
> - The IT outsourcing market to grow 6 percent annually through the end of the decade, reaching $112.5 billion in 2009.
> - The current $33.8 billion U.S. market to grow at 4.2 percent.

Organizations also outsource to access specific expertise that they may not possess and cannot afford to hire full-time—trusting that the outsourced work will incorporate that expertise. For example, if you outsource application programming, you probably expect that the individuals doing this work know about application security and will incorporate it into the product they create for you. You probably also expect them to know how to protect information in a shared customer environment; making sure that the code they create for your organization is not accidentally sent to another customer.

Outsourcing is becoming commonplace, particularly with many top financial, health care, tax reporting, and credit reporting companies. Chances are there are people within your organization considering outsourcing some of your data processing activities.

You Are Entrusting Another Entity to Protect Your Data

When you entrust business partners with your company's confidential data, you are placing all control of security measures for your organization's data completely into their hands. That trust cannot be blind. Many recent security incidents have resulted from inadequate security practices within outsourced organizations handling another company's customer or employee data.

When you outsource critical data processing and management activities, you must take action to stay in charge of your own business data security and minimize your business risks. You must know:

How the business partner is complying with your regulatory responsibilities.

How you can demonstrate to regulators that you are in compliance when someone else possesses your data.

You must hold your business partners to strict security standards. In many instances, the standards applied to business partners will be more stringent than your organization's internal security requirements.

Ensure Your Business Partners Have Strong Security Programs

How you make sure your business partners are taking appropriate actions to protect the data with which you've entrusted them depends upon the situation and existing legal restrictions. The following list highlights general actions you should take:

Require a potential business partner to provide a copy of a recent security audit of their operations that was performed by an independent reputable party. Even if the audit is broad, it will demonstrate they have gone through an audit by a reputable company.

Require business partners to complete a security self-assessment questionnaire, provided by your company, about their information security and privacy program. When creating this questionnaire, structure the questionnaire around the ISO 17799 and OECD topics in addition to any specific regulatory requirements that are beyond these standards.

Include security and privacy requirements within the contracts you have with the business partners. Put in enough detail to cover all issues, but don't be so specific that you allow them a way to avoid doing a security activity just because you did not specifically state it within the contract. Include within the contract citations of the specific laws for which your company must comply so that the business partner understands they must also comply with such regulations.

Require business partner personnel to receive information security training for appropriate security practices prior to handling or accessing your company's information. Don't limit the training to electronic data; if they handle storage media, paper documents, speak to customers about their data, or access data in any other way, make sure it is covered in the training. Require regularly scheduled training and awareness to occur following the initial training.

Review the business partner's information security policies. Include this requirement in your contract with the business partner. Ensure the policies cover all the topics related to the activities the business partner performs for your company. Ensure the wording is strong enough to actually motivate the personnel for compliance. Look for executive endorsement of the policies and for clearly stated sanctions for policy violations.

Require an abbreviated form of the self-assessment, a type of information security and privacy attestation again provided by your company, that the business partner must complete each month or two, have their executives sign, and submit to your company as a requirement of continuing to do business. The signatures and contract language will help to demonstrate due diligence on the part of your company and will hold the business partner to a legal standard of due care.

For business partners handling particularly sensitive and/or regulated information, require a clean-room environment to keep information from walking out the business partner's door.

> ✎ In a clean room environment, all the machines and output devices except for terminals are disabled. Copies of data cannot be made, hard drives cannot be used, mobile computing devices and desktop computers cannot download data from any of the computers, and data is otherwise not available for downloading, printing, copying, or accessing beyond the contracted purposes. The servers reside in your country of residence. There is no way for the information to leave the outsourced company.

Typically in such arrangements the outsourced company's employees are physically searched when entering and leaving. These are very strict precautions, so they will not work for every company, but they definitely should be used if your level of risk warrants such actions.

Limit the amount and types of information the business partner personnel can see and/or access based upon the business needs. For example, if the business partner contracted activity is to verify a customer is a good credit risk, don't send all parts of the application to the business partner; just send the information required to approve the application.

Require criminal and, where appropriate, financial checks to be performed on the business partner personnel prior to their hire. No matter how many security safeguards are in place, it's difficult to stop an opportunist who will steal data for money, revenge, or some other reason. Ensure that the people handling your data have not been convicted of criminal activity that would make them a high risk for handling your data. This verification might be tricky in some countries because records of criminal activity may not be centralized, such information may be labeled differently, and in some countries doing such checks are against privacy laws. As mentioned earlier, and worth emphasizing, make sure the business partner personnel are well trained about security procedures and legal consequences.

Make sure none of your disgruntled ex-employees are now employees of the business partner to which you are outsourcing your data handling. Such situations have had a devastating impact on companies.

Send personnel from your company to visit the business partner sites regularly, or at least occasionally, to view the facilities, meet employees, and monitor employee turnover and subcontracting activities.

Common Business Partner Risks

The following list highlights several areas of recurring vulnerability that have appeared in past business partner security reviews:

The information provided within the business partner's security self-assessment responses might not match the security requirements within the business partner's security policies. For example, the respondent for the self-assessment may indicate the passwords used are a minimum of six characters, but the policy may indicate passwords must all be a minimum of eight alphanumeric characters. Such conflicting information should raise a red flag for you; it may indicate the business partner does not enforce compliance or communicate the security policy requirements to its personnel.

The business partner may be subcontracting the processing of your data to yet another company that does not have good security practices and/or may be located in a different country from yours or the business partner. Be sure to cover this within your contract with the business partner.

The business partner may not have any security policies or controls in place for mobile computing devices (laptops, PDAs, Blackberries, smart phones, and so on) or for their employees who work from home. However, they may have personnel who use these types of computers to process your data. Be sure appropriate security is in place for such situations.

Business continuity and disaster recovery plans are often either missing or were written several years ago and were never tested. Make sure the business partner has up-to-date plans in place and tests them regularly.

The business partner may not have any requirements to encrypt confidential data when transmitting through untrusted networks, such as the Internet. Be sure to require encryption as appropriate to how the business partner transmits your organization's data.

Encryption is often not used to protect information in storage, in transit, or on mobile computing media and devices, such as laptops, PDAs, backup tapes, USB drives, and so on. Be sure encryption is used by the vendor to mitigate the risk involved in such situations, including when the company is storing information from other companies on the same servers as they are saving your data.

The business partner may have been involved with a security or privacy breach. There are multiple services you can use to check on this, in addition to dozens to hundreds of good Web sites to search for news about the business partner and any published security breaches for which it was involved. If you find the business partner had a breach or incident, be sure to ask the company about it and find out what actions were taken to prevent such an event from occurring again.

The business partner may not have procedures in place to securely and irreversibly dispose of data when it is no longer needed or according to data retention requirements. Many business partners simply reformat hard drives or overwrite the drive once as part of their disposal practices. Business partners often also sell their retired computers to recoup their investment, but they do not remove the data from the hardware before doing so. Make sure your organization approves of the disposal procedures your business partner has in place.

The business partner may not have any security controls for sending backup media containing your organization's data to offsite storage and/or they may not have adequate security at the offsite storage site. Make sure your organization carefully reviews the business partner's practices for sending data storage media offsite.

Responsibility Follows the Data

The bottom line is that outsourcing data handling, processing, and management is a risky proposition for your company. It is your responsibility to ensure strong security follows the data to your business partner. You must perform due diligence to ensure your business partners are protecting your data according to your security requirements. You are ultimately responsible for what happens to the data you've given to your business partners.

Be sure to discuss these issues with your organization's legal counsel and acquisitions areas. Modify business partner contracts and acquisition requirements according to what is best for your organization. Don't allow your organization's name to make the headlines because your business partners did not secure your data appropriately and subsequently experienced a security incident.