National Insider Threat Special Interest Group (NITSIG)

Considerations For Outsourcing Work To Third Party Contractors

Considerations For Outsourced Access To Information Assets

Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they just don't have the resources, experience, or capabilities to do it themselves. Organizations may also "Team or Partner" with another businesses to get specific expertise that they may not possess and cannot afford to hire full time. Organizations that outsource application programming probably expect that the individuals doing this work will know about application security and will incorporate it into the product they create. These same organizations probably also expect the individual to know how to protect information in a shared customer environment; making sure that the code created for the organization is not accidentally sent to another customer, and so on.

When an organization entrusts third parties with the organization's confidential data, they basically place all direct control of security measures for the data completely into the hands of someone else. That trust cannot be blind, nor should the giving organization automatically entrust the receiving organization.

When organizations outsource critical data processing and management activities, they must implement measures to stay in charge of their own business data security and minimize business risks. Many organizations indicate the security issues related to outsourcing are a big concern. Alarmingly, it seems few organizations actually address this issue.

How do you know the third party is complying with your regulatory responsibilities? How can you demonstrate to regulators that you are in compliance when someone else possesses your data? You need to hold third parties to strict security standards. In many instances, such standards will be more stringent than your own organization's security requirements.

The measures you take to 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 consider taking:

- Require a potential third party 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 third parties to complete a security self-assessment questionnaire, provided by your company, about their information security and privacy program. When creating this questionnaire, it is an effective practice to structure the questionnaire around the same regulations your business must comply. The same rules should apply to another organization handling your data.

- Include security and privacy requirements within the contracts you have with third parties. Include enough detail that you 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 contracts citations of the specific laws for which your company must comply that the third party must also then comply with.

- Require third-party personnel to have 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 such as paper documents, make sure it is covered in the training. Require regularly scheduled training and awareness to occur following the initial training.

- Review the third party's information security policies. Ensure the policies cover all the topics related to the activities they are performing for your company. Ensure the wording is strong enough to actually impact the personnel activities. Look for executive endorsement of the policies and for clearly stated sanctions for policy infractions.

- Require an abbreviated form of the self-assessment form, a type of information security and privacy attestation, again provided by your company, that they must complete each month, 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 also hold the third party to a legal standard of due care.

- For third parties handling particularly sensitive and / or regulated information, require a clean-room environment to keep information from walking out the outsourced company'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, PDA's cannot get information downloaded 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 measures.

- Limit the amount and types of information the outsourced personnel can see based upon the business needs. For example, if the outsourced company verifies a customer is a good credit risk, don't send all parts of the application; just send the information required to approve the application.

- Require criminal and, where appropriate, financial checks to be performed on the third party personnel prior to their hire. No matter how many safety precautions are taken, 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 may be tricky in some countries because records of criminal activity may not be centralized or such information may be labeled differently. As mentioned earlier, and worth emphasizing again, make sure the outsourcing workers are trained properly about procedures and legal consequences.

- Make sure none of your disgruntled ex-employees are now employees of the organization to which you are outsourcing your data handling. Such situations have led to devastating situations for companies.

- Send personnel from your company to visit the outsourcing sites regularly to view the facilities, meet employees, and monitor employee turnover and subcontracting activities.

- Find out how the third party screens and monitors employees. It is ideal to require that they perform criminal, credit, and reference checks as part of their background check process. However, this is not possible in some countries that do not have a centralized criminal database system. It is also not possible in some countries where doing such checks are against their privacy laws.

- Obtain documentation for how the third party will handle a system breach. Formal breach identification and notification procedures should exist.

- Determine where disputes will be resolved. Have you contractually required that any legal actions will be resolved in your jurisdiction? Make sure you discuss this carefully with your legal counsel.

- Ensure the third party has liability insurance and identify what the insurance covers. If there is a problem that occurs with your information while in the third party's control, liability could rest with your organization—and will likely rest with your organization if the third party is located outside your country.

- Identify the laws and regulations that apply if a system breach occurs at the third party.

- Determine whether your organization's liability insurance covers outsourcing activities.

- Contractually require the third party to obtain your organization's authorization before they subcontract any work that involves your organization's information or access to your systems.

Common Weaknesses

The following list notes recurring vulnerabilities for third parties; be sure to pay particular attention to these:

- The information provided within the vendor's security self-assessment responses often does not match the security requirements within the third party'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 third party does not enforce compliance or communicate the security policy requirements to its personnel.

- The third party 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 third party. Be sure to cover this within your contract with the outsourced company.

- The third party 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 never tested. Make sure the third party has up-to-date plans in place and tests them regularly.

- The third party 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 useful Web sites to search for news about the third-party company and any security breaches for which it was involved. If you find the vendor had a breach, be sure to ask the company about it and find out what actions they have taken to prevent such a breach from occurring again.

- 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 and when the company is storing information from other companies in the same servers as they are saving yours.

Source:

The Definitive Guide To Security Inside The Perimeter EBook - Realtime Nexus
http://www.realtimepublishers.com/book?id=49
Some minor edits were made to original content.

Contact Information
Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
CEO Insider Threat Defense, TopSecretProtection.Com, Inc.
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instructor
Cyber Threat-Insider Threat Risk Assessment Auditor / Analyst
888-363-7241 / 561-809-6800
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com