Security and Privacy Contract Clause Considerations

by Rebecca Herold & Christopher Grillo ***June 2006***

NOTE: Christopher and I created the table found within this article for our two-day workshop now entitled "Effectively Partnering Privacy and Information Security for Business Success." The table has been very helpful for organizations addressing outsourcing and partnering security and privacy issues, so I am making it available here in the hope it will also be helpful to you. For more information about the workshop, in addition to Christopher's biography, please see http://www.gocsi.com/training/erc/pisp.jhtml). - Rebecca Herold

Trust Cannot Be Blind

When you entrust business partners and vendors with your company's confidential data, you are entrusting them with all control of security measures for your organization's data. That trust cannot be blind. Many recent privacy and security incidents have resulted from inadequate privacy and/or 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 demonstrate due diligence, stay in charge of your own business data security, and minimize your business risks. You must know:

> Whether the business partner's information security and privacy program is adequate for handling your organization's data
>
> 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.

Perform Due Diligence

Organizations should plan to perform several activities to determine the adequacy of information security and privacy practices within business partners, vendors, and other outsourced companies. We have performed a significant number of these activities over the past few years, some of which include:

- Requesting the partner to complete a self-assessment information security and privacy questionnaire
- Having an independent party perform an audit of the partner's information security and privacy program and data handling enterprise
- Requiring the partner to obtain a security certification, such as BS7799 or SAS 70 Type II, for the scope of their enterprise involved with handling the entrusted data
- Going onsite to perform an audit of the information security and privacy program and view actual business practices
- Including specific information security and privacy requirements within the contracts with the partners

Contractual Considerations

While performing these activities, we have compiled a listing of issues and important considerations to include within the contracts. The specific items your organization should include will depend upon your organization and the relationship with each of your partners.

As with any contractual activities, it is important to discuss with your legal counsel and choose the requirements and wording that is most appropriate for your organization. Use the following table as a checklist to go over with your legal counsel when discussing new contracts and when reviewing existing contracts to determine whether updates are necessary.

Service Levels		
Contract Area	**Description**	**Notes**
Services to be provided	General commitments of the organization and the third party of the functions to be performed, the deliverable to be produced and the user community to be served.	Ensure services are in compliance with applicable laws and regulations. If required by laws, ensure consent has been obtained from all individuals to outsource personally identifiable information handling to another entity.
Service levels to be provided (Service Level Agreements – SLAs)	The services provided will be in accordance with agreed-upon service levels (usually identified in a service schedule) and whenever possible, using a quantitative tool for performance measurement.	Ensure service levels are adaptable and meet your business requirements. Examples include security service levels for: patches, vulnerability identification, data availability, and incident monitoring and response timeframes. In the event of an outage, how many hours until service will be restored? Define the maximum allowable downtime in a worst-case scenario. Establish standard SLA criteria that must be agreed upon.
Availability of services	Specify requirements necessary to ensure service in the event of service failure.	Include measures to reduce risk of service loss, such as backup and recovery measures, contingency and disaster recovery plans. Contractually require documented backup and disaster recovery plans. Contractually require regular backup and disaster recovery plan tests.
Termination of relationship	Contractually require the business partner to return and/or irreversibly destroy all your company's data, as appropriate, immediately upon termination of your contract with the business partner.	Ensure the business partner does not continue to have access to your company's systems and data when your relationship with them is terminated. Termination of a business relationship presents great risk to your company; this is when the former business partner often stops protecting your data or mishandles it, putting your business at risk.

System/Data Protection Responsibilities		
Contract Area	**Description**	**Notes**
Definition of responsibility	Define responsibilities in all key privacy and information security areas (security administration, technical support, privacy, training and awareness, enterprise program, and so on.)	Contractually require a position or person to be named as responsible for information security and privacy issues and to be the primary point of contact for related communications.
Compliance with relevant laws and regulations	State the requirement of complying with applicable international, national and state level laws.	Spell out desired compliance obligations (e.g., HIPAA, GLBA, and so on). This is standard language to ensure that the vendor adheres to and contractually agrees to support regulatory requirements.
Third party to comply with the organization's security policies and standards	State that the third party must comply with your organization's privacy and information security policies and standards.	Reference appropriate components of privacy and information security policies which may include physical security of premises, clearance of personnel, data security storage, media handling, and so on. Contractually require the third party to have documented information security and privacy policies.
Requiring confidentiality	Contractually require a nondisclosure agreement/confidentiality clause with the business partner and insist that the business partner has confidentiality agreements with relevant staff (anyone who has access to your data) and subcontractors (outsourced relationships, and so on.)	This should be in your standard contract language, typically under "Confidentiality."
Control use of systems and data	Require the third party not to access, use, amend, or replace any application systems, data, software, hardware, or communications systems without prior authorization from a named person or position from within your organization.	Be sure to contractually require that the third party obtains your permission to use production data and purchased data lists for test purposes.
Scope of access permitted	The third party should have the minimum level of access to assets and data to meet the business requirements.	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.

Provide security awareness, training and written guidelines	Contractually 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. Contractually require regularly scheduled training and awareness to occur following the initial training.
Anti-virus policy and procedures	Include a clause to provide protection from viruses and other malicious code.	Due to the high risk from virus and other malicious code infection, include a specific clause requiring the third party to have up-to-date malicious code prevention systems implemented.
Loss of customer data provisions	Ensure that the business partner is contractually required to appropriately protect customer data or face penalties, such as fines, contract termination, prosecution, and so on.	If your business partner loses data your company is still ultimately responsible for the loss of customer data.
Use of data - separation of data	Contractually require your company's data to be protected and separated from competitor data.	Depending on the risk, ask for physical and logical separation of data from other organizations' data — particularly if the partner contracts with your competitors. Document the controls that a business partner must acknowledge and maintain to provide for the protection and separation of data.
System development / change security risk assessments	Contractually require the third party to provide documentation that an adequate risk assessment process was performed during system development and changes to the system.	Security risk assessments should be done as part of the design and implementation of new information resources and during the changes. Contractually require the business partner to provide a copy of, at the least, an executive summary of the most recent risk assessment upon your company's request.
Monitoring requirements and incident response, disclosure, reporting	Contractually require that the business partner monitor for security incidents defined in the business partner relationship and that they provide for the capability to respond to and resolve information security incidents effectively.	Related to this is incident disclosure; require the business partner to immediately report all security incidents to your company, expediting those that involve regulated information such as social security numbers, credit card numbers, and so on.

Personnel exit policies and procedures	Contractually require the business partner to have procedures in place to retrieve all your company's data and information assets from any of their employees immediately upon their termination from the business partner.	It is a high risk when a third party's employees who have been handling your company's data leave their company. This is especially true if the employee was allowed to work from home, used their own personal equipment, kept your data on mobile storage devices, and so on.
Computing equipment disposal	Contractually require the business partner to irreversibly remove all your company's data from all the hardware they retire, sell, donate to others, dispose of, or otherwise no longer use.	Many incidents have occurred when data is not removed from computing equipment that companies have sold, thrown away, or donated to other groups.

Business Partner Privacy and Security Liaison		
Contract Area	**Description**	**Notes**
Third party security function	Contractually require the third party to assign a person to coordinate security responsibilities.	Contractually require the third party to provide upon request the formally documented job description for the position with information security and privacy responsibilities.
Lines of communication	Establish clear lines of communication about information security and privacy with the third party.	Contractually require the third party to identify a point of contact with whom your company can communicate at any time about information security and privacy issues.
Regular review meetings	Contractually require meetings to review service levels and security incidents.	Meet at least once a quarter for business partners who handle customer and/or employee personally identifiable information.

Business Partner Personnel		
Contract Area	**Description**	**Notes**
Suitability of the third party's staff	Contractually require third parties to notify your company of any personnel who used to work for your company.	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.
Recruitment policy and security clearances of the third party's staff	Contractually 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.
Disciplinary procedures	Contractually require the third party to have clearly documented disciplinary procedures implemented that are consistent with your company's procedures.	Make sure the business partner personnel are well trained about information security and privacy procedures and legal consequences. Ensure documented sanctions policies exist.
Subcontractor relationships	Prohibit subcontractor relationships that would provide access to your organization's data or systems unless approved by your company.	Determine how to handle subcontractors. Prohibit subcontractor relationships in contracts and/or establish processes for approval of subcontracting relationships.

Right to Audit and Monitor		
Contract Area	**Description**	**Notes**
Business partner self-assessment requirement (prior to signing the contract)	Contractually require business partners to complete an information 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. Obtain these self-assessments prior to contractually committing to any business relationships, and then periodically following the formal establishment of the relationship.
Right to audit	Contractually require that regular information security reviews be done to ensure that the control architecture and supporting standards, baselines, procedures, and guidelines are being adhered to. Recommend, or better yet require, that the business partner use an independent third party to assess information security and privacy controls.	Contractually require that copies of audits are made available for your review. Types of audits may include: SAS 70 (Type I & II), BS7799 certification audits, vulnerability assessments, penetration tests, and so on. Ensure adequate access to all sites, records, documents, software, and so on. The third party should agree to independent or ad hoc audit inspections during the third party's normal working day with reasonable notice, such as seven to 15 days in advance.
Audit review actions	Contractually require the third-party to respond in writing with action plans arising from audit reviews.	When risks and vulnerabilities are discovered during audits it is important for the third party to provide a written plan for addressing the issues, and a timeline for issue resolution/correction.

Liability		
Contract Area	**Description**	**Notes**
Warranty	Provide the standard contracting language as provided or recommended by your acquisitions department.	Ensure the warranty includes wording for applicable data protection regulatory requirements.
Damages	Provide the standard contracting language as provided or recommended by your acquisitions department.	Include requirements for the third party to reimburse your company for information security and privacy incident damages involving your company's data that occur within their organization, such as if one of their employees loses a laptop with your data, if they lose a backup tape with your data, and so on.
Consequential loss	Provide the standard contracting language as provided or recommended by your acquisitions department.	Include requirements for the third party to reimburse your company for information security incident damages involving your company's data that occur within their organization, such as if a hacker obtains your company's database within their system, and so on.
Insurance	Provide the standard contracting language as provided or recommended by your acquisitions department.	Consider requiring the third party to have cybercrime insurance. Factors to consider are the types of data the third party handles, the geographic locations, the types of activities the third party does with the data, and so on.
Loss	Provide the standard contracting language as provided or recommended by your acquisitions department.	Ensure the amount of loss includes the value of the data and service time, not just the value of the hardware involved.

Other Contracting Considerations

When including information security and privacy requirements within the contracts you have with your business partners include 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 citations of the specific laws for which your company must comply so that the business partner understands that they must also comply with such regulations.

Review the business partner's information security policies. Require within the contract with the business partner that information security policies must be made available immediately upon your company's request. Ensure the policies cover all the topics related to the activities that the business partner performs for your company. Ensure the wording within the partner's information security policy 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.

Bottom Line: Responsibility Follows the Data

The bottom line is that entrusting your data to another company, or outsourcing data handling, processing, and management, is a risky proposition for your organization. It is your responsibility to ensure strong security follows the data to your business partner and that safeguards remain during the duration of the business relationship.

You must perform due diligence to ensure your business partners are protecting the data according to your information security and privacy requirements. Remember, you are ultimately responsible for what happens to the data you've given to your business partners.

It is worth emphasizing that you need to 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.