# Third-party service providers in data security

Many companies outsource the management and control of all or some of its information systems, networks or data storage to service providers and cloud-based services. Third-party service providers include ISP providers, hardware, software and firmware vendors and other third-party providers who perform services on behalf of your company and may have access to sensitive data. From a business standpoint, business owners should always assume third-party services are vulnerable. As a result, they should develop a formal written process for selecting and managing third-party contractors and services. Risk control considerations include, but are not limited to:

## General considerations for selecting a contractor or service provider

- Evaluate their financial stability.
  - Is this an established company or a start-up?
  - Do they have adequate financial solvency to provide long-term support?
- Confirm they are staffed to provide an acceptable level of customer technical support.
  - If required, can they provide 24/7 support 365 days a year?
- Determine the credentials of the personnel who will be assigned to your contract.
  - Specify the security background checks that you will perform before retaining a third-party.
  - Do they have the technical expertise to complete the project or service?
- Describe the security background checks and qualifications of the personnel who will have access to your information.
- Determine if they will handle all portions of your contract or if they will need to sub-contract with other companies.
  - Describe any services they will sub-contract.
  - If they sub-contract to others, verify they are assuming responsibility for ensuring their sub-contractors comply with all your security requirements.
- Conduct and obtain enough information e.g., internet search, independent surveys and reports to get a better understanding of their advertised services/operations.
- Obtain references from other customers or organizations such as the Better Business Bureau.
- Ask them to describe their history of cyber security incidents and improvements they have made.
- Confirm they are knowledgeable of, and in compliance with all legal and regulatory requirements.
- Ask them to describe their business continuity capabilities.
  - Do they have a written plan? And, is it practiced at least once a year?
  - Do they have redundant systems and/or data storage sites?
  - How quickly can they resume normal operations in the event of a failure at one location?
- Ask them to describe their cyber incident response plan.
  - In the event of a breach, what is their normal process for investigating, responding and notifying your company?

## Contract terms and conditions/risk transfer

When contracting with others, draw clear lines of responsibility so there is no question whose job it is to safeguard sensitive information. All contracts should be signed before beginning the work or service.

- Establish internal policies governing your contractual risk transfer program specifying the individuals within your company who have authority to make or approve changes to contract provisions and insurance requirements.

# Third-party service providers in data security

- Work with an attorney knowledgeable in contract law to develop effective wording. The contract terms and conditions should consider risk transfer agreements, including, but not limited to:
  - The contract should include hold harmless, indemnification, and defense clauses to protect your company's interests. If you are being required to indemnify other parties, you should require your contractors to assume those same duties.
  - Insurance specifications should be listed within the contract, detailing coverages, coverage limits, additional insured status, written notice of cancellation clause, etc. Consult with your insurance agent for specific details.

**Data security requirements**

Your contract should include acceptable use agreements that limit how the third party may access or use sensitive data and systems, and disciplinary consequences for noncompliance. Provisions should include, but are not limited to:

- Minimum qualifications and certifications of personnel who are working on the project or service, including the successful passing of security background checks for any personnel having access to sensitive data or critical systems
- A list of individuals authorized to access your system or data and a statement that the contractor is responsible for properly protecting and controlling administrative privileges. The list should be maintained with updated information
- Specifications requiring strong password controls
- Contractor responsibility for ensuring its subcontractors comply with all security requirements
- Contractor responsibility for meeting all legal and regulatory compliance
- Specifications that work produced by contractors is owned by your company
  - As appropriate, this work should contain a copyright notice that reflects the ownership
- Restrictions on types of information accessed by the contractor and its subcontractors
- Provisions that they will protect the confidentiality and integrity of the data in their care and custody; depending on the sensitivity of information, confidentiality clauses and nondisclosure agreements may be required
- Restrictions on copying, storing or transmission of data
- Requirements for the return or destruction of information and assets at the end of the contract or job
- Specifications to require maintenance of physical security and access controls to restrict access to authorized users only

**Business continuity requirements**

Your contract should include business continuity requirements, including, but not limited to:

- Specifications on an acceptable level of customer technical support such as response time, time period available per day or days open per week
- Specifications on the maximum amount of response time allowed to replace or restore your critical equipment, applications, software or services in the event of physical damage or cyber breach

**Incident response requirements**

Your contract should include incident response requirements, including, but not limited to:

# Third-party service providers in data security

- Specifications on the notification procedures to your company of any security incidents and requirements for managing the incident
- Requirements that they will cooperate as needed in support of your incident response plan

**Audits**

To ensure that your contractors are diligent in the services they provide to protect your data, your contract should specify your right to conduct audits.

- State the frequency and level of security audits they must conduct (e.g., self audits or certified third party) and the audit report details they must provide
- For third parties that store your sensitive data, include a requirement that they record all authorized access to the data and any unauthorized attempts to access the data. Information such as the date, timestamp, source address, etc., should be logged and provided to you in scheduled reports. See the Travelers Risk Control bulletin *Map and secure your network* for more information
    - Require they comply with all legal, regulatory and contractual requirements

## Outsourcing – signing contracts of others

Many companies outsource the management and control of all or some of its information systems, networks or data storage to service providers and cloud-based services. Typically for these services, you are required to sign their contract, which is typically one-sided to the benefit of the outsourcing company. The contract should be reviewed by your legal counsel and changes made as necessary to protect your interests.

## Open source software – caution

Open source software can potentially present significant risk in many forms, including to operating systems, platform elements, development tools and middleware. Many proprietary software programs contain open source components. Contrary to common misconceptions, most open source software is still subject to licensing agreements, imposing specific obligations on anyone who uses, modifies or distributes the code. If the open source software developers disclaim responsibility associated with the software, the user may be responsible for any claims that the software violated third-party copyrights, patents or other intellectual property rights.

**For more information about Travelers Canada, visit our website at travelerscanada.ca, contact your Risk Control Consultant or email Ask-Risk-Control-Canada@travelers.com.**



Travelers Canada, Suite 200, P.O. Box 6, 20 Queen St. West, Toronto, Ontario M5H 3R3