WeirFoulds LLP

Managing cybersecurity risk in contracts

Many companies acquire IT services from third-party service providers where the service providers host or otherwise acquire data and other confidential information of a company. In this context, software services "in the cloud" may involve hosting by the service provider of a company's data and other confidential information. The service provider's standard form contract will typically seek to minimize its risk regarding breaches of a company's confidential information.

Take this quiz to find out how prepared you are to deal with IT service contracts where the service provider will handle data and other confidential information of a company.

GO TO *CANADIANLAWYERMAG.COM* TO WATCH A WEIRFOULDS LLP LAWYER TALK ABOUT THIS QUIZ.

1 You flip to the section of the agreement that deals with confidentiality and you see that the "standard of care" is that the service provider must maintain the same degree of care regarding safeguarding the data and other confidential information supplied to it by the company that it applies to its own confidential information. You have seen this standard of care before and noticed that it is quite common. What is the best provision to add in order to help ensure that the service provider is responsible for all security breaches of the company's data?

(A) The right to inspect the service provider and its facilities.

(B) An additional standard of care.

(C) Incident notification and management procedures in the event of a security breach.

(D) Tight restrictions upon the service provider's use of subcontractors.

2 Which one of the following items is relevant to contracts and cybersecurity?

(A) ISFA Standard 6240.

(B) CSA 683-41A.

(C) INFA EEC Data Standards.

(D) SSAE 16.

3 You are successful in negotiating robust confidentiality obligations in order to ensure that the company will be able to recoup all of its losses in the event of a breach by the service provider of confidentiality obligations. You negotiate an indemnity from the service provider regarding any breach of the obligations.

You are happy because the indemnity is very broad — for example, it includes indemnification of the company's affiliates, officers, directors, employees, etc., and covers all direct and indirect losses and damages suffered by the company and not merely indemnification for third-party claims. Is your work done on the contract in order to ensure full recovery for breach of the confidentiality provisions?

(A) Yes.

(B) No.

(C) It depends on the contract.

4 What other provisions should a company insert in an IT service contract in order to manage cybersecurity risk where the service provider possesses the data of a company?

(A) Restrictions on location of the company's data.

(B) Traditional insurance must be maintained by the service provider.

(C) Security schedules.

(D) Some but not all of the above.

WeirFoulds LLP

QUIZ ANSWERS

1 **(B)** A "strict liability" standard of care may be imposed; in other words, the confidentiality provisions could be amended to add that the service provider will not disclose the confidential information of the company and must keep it strictly confidential — by doing so, the service provider is liable for a breach of confidentiality even if it complies with the standard of care regarding safeguarding the confidential information. The other provisions mentioned such as inspection rights are useful, but the key provision is the standard of care.

2 **(D).** (A), (B) and (C) are fictional. SSAE 16 (Statement on Standards for Attestation Engagements Number 16) are audit standards established by the American Institute of Certified Public Accountants that contain provisions geared toward service organizations such as IT service providers. Audits are obtained by service providers to, among other things, help demonstrate that they have adequate contracts and safeguards when they host data belonging to their customers.

Service providers are often reluctant to provide security audit rights in favour of a company. As an alternative, the company will gain some comfort if the service provider obtains and provides to the company third-party audit reports prepared in accordance with third-party standards such as SSAE 16 audit standards. The contract could include a provision that such reports are provided to the service provider. This SSAE 16 standard provides for "SOC 1 Reports", "SOC 2 Reports" and "SOC 3 Reports", and the reports fulfill different functions.

3 **(C)** It depends on the contract. The service provider's standard contract will typically contain limitations and exclusions of liability in the service provider's favour. They usually consist of a "monetary cap" regarding all liability under the contract (often expressed as a total of fees paid to the service provider over a certain period of time), and an exclusion regarding consequential and indirect damages that may include an express exclusion regarding loss of data. Many IT service contracts are drafted so that the limitations and exclusions of liability apply to indemnities and, therefore, a robust indemnity may in fact be undermined. A company may seek to negotiate "carve-outs" regarding the exclusions and limitations of liability that apply to breach of confidentiality provisions and indemnification for the breaches.

With respect to the "monetary cap", a service provider may not be willing to accept a carve-out that provides for unlimited liability, but the service provider may accept a substantially higher monetary cap than with other contractual claims. It depends upon the bargaining strength of the parties. It is important to pay attention to the express provisions of a force majeure clause so that it is clear the extent to which, if any, the service provider may avoid liability for cybersecurity risks notwithstanding any other provision of the contract.

4 **(D)** All are useful except for traditional insurance provisions. Traditional insurance policies do not cover data loss or damage due to a security breach. "Cyber insurance" is an evolving form of insurance that is helpful with respect to security breaches. Cyber insurance is especially important if the service provider is a small company that may not be in a position to adequately compensate the customer for a loss.

Provisions may be inserted so that data may be hosted only within a specified geographic area, putting the company in a position to assess the risks. If the data is hosted outside of Canada, the company should consider, among other things, whether the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure (especially if the data includes personal information) that are sufficiently rigorous.

The agreement may contain one or more security schedules that deal with IT security requirements and policies (data storage, data retention, malware protection, etc.) that help manage security risk.

YOUR RANKING?

- **One correct:** *might be time to brush up*
- **Two correct:** *not bad, but some further work needed*
- **Three correct:** *very well done, but not perfect*
- **Four correct:** *excellent*