Limit Your Risk of Data Breach Liability: 13 Important Considerations Before Providing Data to a Third Party

Description

By Colin Coleman, John Ottaviani, and Brian Reilly

Does your business provide company or customer data to any of its vendors? If so, do you know what contractual provisions are in place to protect your business in the event of a data breach by your vendor?

Vendors typically try to limit their liability under their contracts and seek to minimize exposure in the event that they experience a data breach. Entering into a "standard" agreement without carefully reviewing the data privacy provisions could leave your business with the unenviable task of complying with data breach notification laws and shouldering remediation expenses, even though it was not your business that was compromised.

Although any vendor can suffer a data breach, you may be at a heightened risk if you contract with vendors for such things as: (i) cloud back-up services, (ii) outsourced IT services, (iii) online sales management, (iv) payment processing, (v) order fulfillment, (vi) billing processing, or (vii) records storage and management.

Having a comprehensive cyber liability insurance policy in place can provide your business with some protection against loss, but no insurance policy can force a third party vendor to provide you with indemnification, information, or cooperation. For that, you need to have contractual provisions in your favor.

Here are 13 things to consider before entering into any contract that provides a vendor with access to your company's or your customers' data.

1. Does the vendor carry cyber liability insurance, and if so, what are the limits and can the vendor provide you with an insurance certificate?
2. Does the contract contain an affirmative duty to notify you immediately in writing if a data breach has occurred?
3. Is the contract clear as to what constitutes a breach and the scope and extent of the required notice to you?
4. Is there a cooperation clause in the contract that obligates the vendor to cooperate fully with you in the event of a data breach?
5. Does the contract provide you with access to a senior level point person at the vendor to manage the notification process?
6. Is there language in the contract that obligates the vendor to provide you with continuing updates following a data breach?
7. Does the agreement allow you access to information sufficient to allow you to protect your business and customers and to comply with any notice and remediation obligations?
8. Does the vendor have a written data breach incident response plan and written information security program?
9. Is cyber liability risk carved out from any limitation of liability clause in the contract so that any damages your business suffers are covered up to the limits of the vendor's cyber liability insurance policy?
10. Is there a clause in the contract giving you the right to request annual updates of the vendor's cyber liability insurance certificate and compliance with other data privacy laws and regulations?
11. Does the contract contain representations and warranties regarding the vendor's legal compliance standards and obligations, and ongoing obligations of the vendor to comply with all laws relating to data privacy and security?
12. Does the agreement require the vendor to indemnify you if it suffers a data breach?

13. Does the contract include a limitation on the vendor allowing other third party vendors to access or hold your data or that of your customers without your consent?

While the level of detail that you will require in any vendor contract will vary depending on the type of contract and the level of access the vendor has to sensitive data, ignoring these questions or assuming that you are protected could leave your business vulnerable should your vendor suffer a data breach.

Note also that many vendors will require you to accept certain terms and conditions when creating an account or using a service for the first time, rather than signing a formal contract. In these instances, it is unlikely that the vendor will modify its standard terms and conditions for an individual customer, but it is still important for you to understand the cyber-security and data privacy risks before you agree to be bound by the vendor's terms of service.

If you would like help reviewing your current vendor agreements or are entering into a new vendor contract and want to protect your business, contact Colin Coleman, John Ottaviani or Brian Reilly today.

Date Created
February 21, 2019