When you outsource IT functions to vendors, you may entrust sensitive data to these third parties. As the "data owner," your small business is at risk if its data is breached while in the vendor's care. Depending on the particular contract wording negotiated with a vendor, this exposure may be amplified or mitigated. The following outlines some contract areas you should pay special attention to in order to mitigate risk.

Q1. What contract provisions are most important to consider when assessing the risk in outsourcing IT functions and the handling of sensitive data?

Four contract areas can be particularly critical:
- Indemnification clause
- Caps on damages
- Limitation of liability
- Disclaimer of consequential damages

Q2. What is an indemnification clause?

At its most fundamental, an indemnification is an agreement whereby one party agrees to assume the liability of another in the event of a loss. In a typical vendor contract, it is the wording that would enable a small business to seek reimbursement for amounts it is forced to pay to a third party because of damages caused by the vendor. Some indemnification clauses include caps on damages. This means there are limits on the amount of financial compensation a person can receive during a claim, even when the claimant is justified in his suit. This should be a red flag: Even with favorable indemnification wording, caps on damages can significantly reduce the amount of damages a small business can recoup.

Some examples of indemnification wording you may encounter:

Example 1 does NOT include a cap on damages:

Example 2 places a specified cap on damages:

Example 3 places a cap that cannot exceed the amount paid for services:

Q3. What is the limitation of liability?

A limitation of liability clause permits contracting parties to reduce or eliminate the potential for direct, consequential, special, incidental and indirect damages, should there be a breach of contract. The following is an example of such wording:

Except for the payment obligations for a party’s liabilities resulting from a breach of confidentiality or from infringement of the other party’s intellectual property rights or the other party’s intellectual property rights by such party, to the maximum extent permitted by applicable law, in no event will either party have any liability, contingent or otherwise, for any indirect, special, incidental, consequential, punitive, statutory or exemplary damages in any way arising out of or relating to this agreement, the platform or any products or services provided hereunder, including, but not limited to lost profits, lost data, loss of goodwill, work stoppage, equipment failure or malfunction, personal injury, property damage or any other damages or losses, even if a party has been advised of the possibility thereof and regardless of the legal or equitable theory (contract,
tort, statute, indemnity or otherwise) upon which any such liability is based.

Optimally, a small business should reject any attempt by the vendor to limit its own liability and should delete limitations of liability provisions from a vendor’s contract.

Once customers are notified that their information has been breached, they are understandably concerned and upset. Damage control is critical to mitigate the impact of a breach both on the victims and on your business’ reputation. Consequently, it has become standard for businesses that suffer a breach to set up a call center to handle questions and issues that arise post-notification and to provide services such as free credit monitoring for victims.

Customers who are very upset and suffer financial repercussions from the breach may want to sue. In that case, you can add additional fees to hire an attorney to review the case, legal fees if a claim is involved and even legal liability damages to the cost of a data breach.

Q4. What is a disclaimer of consequential damages?

Consequential damages are damages that are not direct, such as the lost business income a small business could face from a data breach or network interruption caused by the IT contractor. If a contract includes a disclaimer of consequential damages, it could eliminate the possibility of seeking reimbursement for these indirect losses.

Small business owners are wise to reject any attempt by a vendor to include a waiver of consequential damages provision in their contract. Second best would be including a mutual waiver of consequential damages, whereby both the small business and the vendor waive their rights to seek incidental, indirect, and consequential damages. An example of a mutual waiver of consequential damages follows:

Neither the Contractor or the Owner shall be liable to the other or shall make any claim for any incidental, indirect or consequential damages arising out of, or connected in any way to the platform or this Agreement. This mutual waiver includes but is not limited to loss of use, loss of profits, loss of income, loss of reputation, unrealized savings or diminution of property value and shall apply to any cause of action including negligence, strict liability, breach of contract and breach of warranty.

Information Security and Privacy Liability Insurance products are available in some states on an admitted basis. The descriptions contained in this communication are for preliminary informational purposes only and coverages are available in the US only on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded by the products described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk.

For more information contact your insurance agent or go to: www.beazley.com/pe.

Other steps to take

Be diligent in assessing the wordings in contracts with potential vendors and --- as much as possible -- choose vendors who provide the most favorable wording.

Information security and liability insurance can also address this third-party exposure, and you can collaborate with your broker and underwriter to evaluate this exposure when weighing how much coverage to purchase. It is a good idea to include copies of a potential insured’s contracts with your submission so underwriters can get an accurate understanding of the exposure. Any contractual provisions for the vendor’s data security measures are also useful to point out. Underwriters like to see that a small business and its vendors are taking data security seriously!

For more information contact your insurance agent or go to: www.beazley.com/pe.