

Do Your Contracts Have Booby Traps? Are You Sure?

Lee Thornbury J.D.

Do Your Contracts Have Booby Traps?

Are You Sure?

By Lee Thornbury J.D.

Virtually any IT contract signed in the 20th Century is a potential landmine for your corporation. Some of those negotiated in the 21st Century are risky, too.

Two primary conditions contribute to the uncertainty—phenomenally fast-paced changes in the IT industry and legislation that requires senior executives to accept personal responsibility for the financial reports of the corporations they manage. Last month in this space we outlined the potential impact of the Sarbanes-Oxley Act on IT and procurement executives. This month we examine steps you need to take to protect yourself and your corporation.

Although Sarbanes-Oxley requires the top brass to sign financial reports those executives depend on the veracity of information and reports supplied and prepared by subordinates. Not the least of these are the data supplied by your organization. The risk is compounded because the suppliers and vendors with whom you deal are outside of the corporation's direct control.

There are innumerable nightmares that can arise in the relationship between a business and its vendors. Not long ago the debacles at ChoicePoint and LexisNexis were front-page news. And we haven't heard the end the end of those and similar deals in which the vendor was less than honest.

What can Information Technology and procurement professionals do to protect themselves and their companies against impending disasters? Start by taking the time to put a good contract into place—one with comprehensive and self-protecting clauses that shield your company and give you options. Too often, in the rush to get the work under way, important contractual protection can be thrown to the side, leaving your company vulnerable when the going gets rough. And it almost always will.

And, once you have a good contract in place, review and update the agreement at least every five years. Make sure your contracts are up-to-date with contemporary business culture and legal trends. Amend, amend, amend, and if the vendor won't cooperate, re-evaluate the financial and legal risks and exposure that an outdated, incomplete contract might cause your company. Take a hard look to determine if you want to keep doing business with that vendor.

Why review contracts that have been in place for years?

Think about the first software contract you read in 1985 (assuming you were reading contracts in 1985). Most likely, it said four things:

- Here's your one piece of software,
- If it breaks we'll replace it,
- You'll indemnify us for everything, and
- Don't make any copies.

It didn't say anything about Y2K compliance to ensure that it kept working. It didn't define "confidential information." It didn't state who owned any work-product generated out of the stuff. Assuming that the software is still being used, are you sure you want to be operating under this agreement?

It continues to surprise me how many companies do not re-examine their contract portfolio on a regular basis. Granted, time is always at a premium; with all the new toys on the market and with all the new vendors, it may seem like a waste of time to go back over moldy old contracts for outdated language and stuff. Or to see the impact of newer rules and regulations. Why bother? Because what you don't know can come back to bite you.

Believe it or not, until a contract is terminated or replaced by agreement of the parties, the original terms, conditions and language most likely will govern the relationship. Even if the parties have been operating under a "working relationship" or "a gentleman's agreement" for years, those new rules and understandings, in most instances, will not prevail over written terms in a contract signed by both parties. This is traditionally known as the Four Corners rule of law. A court will only look to the four corners of the paper to see what governs the agreement of the parties. Any peripheral or extra information that is not included in that contract is nice, but generally doesn't control in the event of a dispute.

Bottom line—if it is not in writing and signed by authorized representatives of both parties, it doesn't count.

Bottom line, part two—a contract is a living, breathing document, and can be changed by agreement of the parties (in writing, of course!) at any time subsequent to the original signing. In this respect, a contract is similar to our Constitution, which has been amended 27 times to reflect the changes and events in our common history during the 217 years since it was adopted (in 1788).

Why review contracts every five years (at least)?

Think about all of the new laws and regulations that directly affect how companies do business. In just the past few years we have seen passage of the Gramm-Leach-Bliley Act (protecting consumer privacy and data), the Health and Insurance Portability and Accountability Act (commonly referred to as HIPAA), Sarbanes-Oxley and the federal Telecommunications Act. Who knows how many state laws and regulations dealing with privacy of personal information, consumer data have been added to the law books? If your company does business internationally and/or on the Internet, international rules and laws can apply to you too.

Now think about this: do all of your company's contracts with vendors, whether for software, services, or materials, include "personal information" in the definition of "confidential information?" Do your agreements with vendors provide a specific warranty that the vendor will take all precautions against potential security breaches? Does every contract have a provision that, in the event a security breach occurs, obligates the vendor to cooperate with you in the investigation, mitigation and correction of the breach (including revealing any pertinent information about their own employees that might fix the responsibility on the vendor)?

Are your vendors responsible for the conduct, good and bad, of their employees and subcontractors while they are on your company's premises or using your company's property, a vehicle for example? If a vendor's products are used correctly but produce erroneous results, who's responsible? Under Sarbanes-Oxley rules your company—more specifically your senior

executives and board members—are looking at financial penalties and jail time for non-compliance with its requirements. Is your vendor contractually bound to step up to the plate and take responsibility for their error?

And finally, is your company in compliance with its obligations and responsibilities under the contract? For example, are unauthorized copies of software being used within your company? Has hardware been “lost” in moves between buildings? Are you required to notify the vendor in the event your company merges with another, or acquires other companies, or changes company names or the state in which it is incorporated? Is the information in the “notice” section of the agreement still accurate as to names, addresses, numbers and so on?

Examples of corporate disasters, big and small.

If you’re not yet convinced of the risks you face every day consider these illustrations of potential corporate catastrophes.

Example No. 1: your company outsources its call center activities to a telemarketing firm. A disgruntled call center employee decides to make some extra cash by copying and selling your customers’ personal information (credit-card PIN numbers). The vendor fires the employee and notifies your company of the security breach. Does your company have any recourse against the call center, in the event that your customers are harmed by the security breach? Who pays for the expenses incurred in notifying your company’s customers of the security breach? When the state Attorney General threatens to sue your company for deceptive trade practices and breaches of the state’s telemarketing laws, will your company be left holding the bag, or can the call center be forced to defend and indemnify you?

Example No. 2: a company that specializes in data mining and consumer profiles licenses sensitive personal consumer information, such as individuals’ social security numbers, bank and credit card account numbers, and credit scores, to others. The information company discovers that one of its licensees is not a legitimate business. The licensee has been selling consumer personal data to all sorts of shady characters and businesses that use the information for identity theft and credit card fraud. Is there potential liability for the information company? You bet. Public disclosure under Sarbanes-Oxley? If it’s a public company, yes. Think this will affect the data company’s bottom line? Without a doubt. Think this is an unlikely real-life scenario? Ask any number of data collection companies, starting with ChoicePoint and LexisNexis, who encountered this exact set of facts in the spring of 2005.

Example No. 3: your company hires an advertising agency to produce a campaign promoting your company’s services. The agency takes care of hiring models, paying dues to the appropriate unions and places your ads on prime time TV. Great reviews, everybody’s happy. Except...five months later, your General Counsel gets a registered letter from a law firm whose name is not familiar. Turns out your advertising agency not only didn’t pay the models, but they also didn’t pay the union dues or the TV stations for the advertising time. Your accounting department verifies that the ad agency presented an invoice, stating that it had already paid these folks and wants reimbursement. The agency even had supporting documentation in the form of invoices from the other suppliers. Further, the check your company issued to the ad agency for “reimbursement” of these expenses was cashed three months ago. Does this mean your company may have to pay the models, unions and TV stations too?

In all three examples, the answer lies in the contract language between the company and their vendor.

Protect yourself—find the booby traps before they explode

These are only three of the countless booby traps that lurk in your corporation's aging procurement contracts. As the trend toward legislative protection of consumer and investor rights picks up pace, the consequences for failure to take action only will increase; and ignorance is no defense.

Prudent IT and procurement executives have initiated systematic portfolio reviews to protect themselves and their corporations. Constant vigilance of and familiarity with your company's contract portfolio is the best form of preventative maintenance in your on-going relationships with vendors. In the same way you change the oil on your car to maintain its warranty, you need to keep fresh and refresh your company contract portfolio. Especially because, unlike your automobile, there is no warranty on your contracts—unless you inserted self-protecting clauses and options when the contract was negotiated.

Maxelerate's goal is to help Sourcing, Procurement, Purchasing, Engineering, IT and other professionals in all industries and government agencies to get better deals from suppliers. We accomplish this by providing Consulting, Training, Seminars and Leadership Implementation.

To get more information about us and find out how you can get better results contact us at:



1600 Golf Road, Suite 1200
Rolling Meadows IL 60008
Phone Toll Free: (866) 855-5335
Phone Direct: (847) 483-5014
Fax: (847) 483-5015
e-mail: BusDev@maxelerate.com