

ARI KAPLAN

## Legal Links For Your Supply Chain

**F**OR THE PAST FEW weeks, my mother-in-law has been eyeing a certain technology stock, waiting for it to reach her strike price. To monitor the markets, she uses a tracking service that streams quotes on her cellular phone. If you offer a service like this — one that requires data from an unrelated third party — be sure to structure your arrangement wisely to ensure your protection and your customers' satisfaction, especially if you count my mother-in-law among them.

IT managers aren't always involved in these business or legal discussions. But they should be, especially when data access is at issue.

Before these talks begin, a nondisclosure agreement must be signed. This will preserve confidentiality and protect trade secrets, which may include the design of your proprietary systems to which the data feeder may have access.

If copyrighted data is being offered

to you, require proof that your counterpart owns all of the intellectual property that's subject to the transaction. And while you're at it, secure a warranty on the functionality of the application being shared or accessed. Make sure it's scalable, too. (This is key for emerging growth companies that could have 1,000 users one month and 100,000 the next.)

In your agreement with the third party, clearly state who owns the final application. Ownership of the end result can be tricky because some programs require extensive maintenance, which may prove difficult for a limited in-house team to handle. Nevertheless, possession has significant control-related advantages.

If you're offering your customers data that they will rely on to make important decisions such as stock purchases, you could expose your company to certain liabilities. (I don't want



to even think about the call I would get from my mother-in-law if she bought her stock at the wrong price because of a misquote.) CIOs should therefore require assurances against, as well as indemnification for, any incorrect data (not including market fluctuations, of course) in any contracts they sign.

Supply chain pacts should require that the networks on which information travels are secure, and they should contain more detailed provisions that outline cyberterrorism contingencies specific to your business. In the event of a cyberattack, try to obtain preferences for your systems so you will be the first to get the data once the feed has been repaired.

Be aware that developers can build time-activated codes or periodic re-authorizations into their work. This is designed to give them the option of turning off the feed when you don't

live up to your end of the bargain. Although it's typically a last resort and requires notice of its use, it can happen. You should, therefore, address such limits upfront.

Disagreements can also arise, so include a dispute-resolution provision. In the modern environment, cost- and time-conscious CIOs may want to consider online alternatives. They can be faster, more efficient and don't require long-distance travel or litigation.

Perhaps most important in managing risk is obtaining comprehensive insurance that provides for all contingencies. Companies should also build redundancy into their systems so that they always have a backup supplier of critical items.

Ultimately, entering negotiations in good faith and with reasonable expectations is the key — anything to avoid that call from my mother-in-law. ▀

### WANT OUR OPINION?

 More columnists and links to archives of previous columns are on our Web site: [www.computerworld.com/columns](http://www.computerworld.com/columns)