Reality Check

Will We Ever Learn?

By Dick Lee

Attempts to link CRM to September 11th show a terrifying lack of understanding of how and why CRM works.

First it was the airlines. Next insurance companies. Then this business sector. Then that one. And finally it's the CRM industry's turn to attempt to cash in on September 11th. We have Experian touting the viability of using credit data to spot potential terrorists. Then we have Siebel Systems reframing its CRM application as a homeland security tool. And more. All lining up to show how their wares can identify potential terrorists as readily as they identify potential customers. All demonstrating that their eagerness to sell their stuff surpasses their knowledge of what makes CRM work—and not work.

Take the credit file approach. To avoid getting arrested myself, I'll refrain from identifying all the data variables in credit databases that might go into profiling a potential terrorist. Of course, up on the Internet, Fair Issac is already selling consumers (terrorists included) the "code" for scoring mortgage applications, allowing clever folks to manipulate their profiles. But no matter. It's more fun (and more profitable) to assume that terrorists are too myopic to avoid behavior that will trigger flags in a credit database—than it is to recognize how fallible our database profiling systems remain. Heck, the credit card industry that relies on credit data like a crutch still pre-approves infants and pets. And we're supposed to feel safer with these data watchdogs on patrol?

Not to belabor the point, but anyone who's been in CRM a day or two likely knows that database analytics work far better at screening *out* than screening in. In other words, they're much more helpful for identifying who's not a terrorist, than who is, which isn't much help at all.

As for Siebel Systems' transformation into a homeland security company, well—I guess what kinda company they are sorta depends on which sales pitch you're in. But Tom Siebel himself did free up some of his valuable time to testify before a Congressional committee about how his software could catch the bad guys. Reading his testimony made me wish I'd saved one of those silver sheriff's badges from my youth so I could run up and pin it on Tommie's chest, his testimony was so eager and

earnest. But better I should dredge up a few thousand case studies of failed CRM implementations that demonstrate what would happen if the government runs off half-cocked and buys CRM/homeland security software on the spot.

You know the case studies I mean. The one about companies too arrogant to consider what their customers want, too fearful to step between feuding functional silos to fix their convoluted workflow, in too much of a hurry to re-engineer work processes—but ready to spend a gazillion dollars on CRM software, which they do, only to experience CRM failures of the first order? So what's so different about our government? It has to adopt security policies palatable to citizens, or they won't last. It has to bring feuding departments together in order to redesign workflow around these new policies. It has to re-engineer work processes to match the new workflow—and to identify specifically what functionality information management/automation software has to provide. And only then can it rationally decide which software applications will work—and which won't. And we're trying to persuade government to buy technology as a first step?

When will we learn? Or perhaps the better question is, "When will we care?"

Dick Lee is Vice President of Minneapolis-based consulting firm Caribou Lake and heads its Customer-1 practice, which specializes in helping clients achieve customer-centricity. Dick is the author of two seminal CRM books—Strategic CRM: the complete implementation manual *and* The Customer Relationship Management Survival Guide. *He also speaks internationally on CRM topics. You may reach him at dlee@cariboulake.com or visit the Caribou Lake website at www.cariboulake.com.*