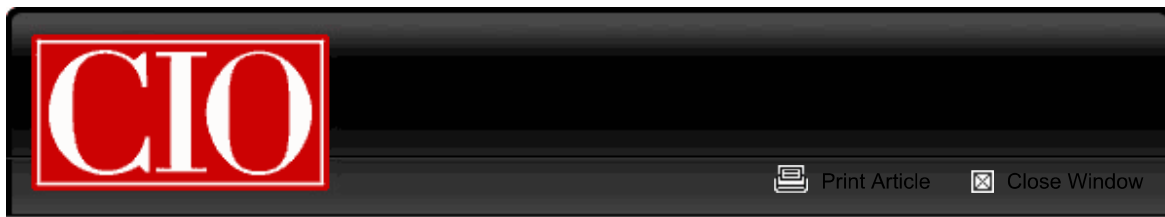


**TECH BRIEFCASE**

Search, store, and share IT white papers from across the web.

Available on the App Store

**NEW APP**



From: [www.cio.com](http://www.cio.com)

## How to Get Smarter About CRM Security

– David Taber, CIO

**May 13, 2011**

If Value Engineering is the identification of different implementation strategies to achieve the business goal, the ultimate in value engineering is to identify requirements that don't need to be done in the first place. Although security and access control would seem to be a poor candidate for this kind of requirements elimination, in many situations the technical solutions are so clumsy and expensive that there's almost no ROI.

This can be politically touchy, as nobody wants to be the one to say "no" to risk reduction and compliance. This can be a particularly pointed issue with CRM systems, which tend to be the most politically charged of any Enterprise application. So... don't say no — instead say "that won't be effective."

### Keeping the users to their own knitting

Let's start with an example: sales' ability to see and change opportunity records in the CRM. The starting point is typically "a sales person should see only the deals that they own and the deals of those that report to them." This is easy to understand, and clean to implement in CRM systems. Sometimes there will be a plot complication — "the reps should be able to see that another rep's deal exists, but not be able to see any of the details." CRM systems can handle that kind of exception without too much trouble.

But in large, multi-channel organizations, there are territory overlays and named accounts. Consequently, it gets harder to automatically determine what a sales rep is supposed to "own." Their territories may have "holes" in them, and even if they don't, multi-national customers present a challenge to the "rep ownership" rules. For example, if GM Canada is making a purchase but the decision is being made in conjunction with GM USA, which rep owns it? This becomes much more complicated when selling to government contractors, where different projects within the same customer business unit may be "owned" by different sales reps.

Enforcing what started as a simple rule now would now take a complex series of lookups and exceptions. And of course, no CRM system has this processing built in: you must custom code it. But

the bigger challenge is maintaining the lookup table(s) that have to be changed every time there's a new rep, new partner, or customer merger or divesture. Sure, you could create a nice UI to maintain and test all the moving parts, but in large organizations the code and lookup tables won't be maintainable. Consequently, the security infrastructure will eventually give somebody the wrong level of access, and it's likely to irritate a fair percentage of your users.

Perfectionism in this kind of issue doesn't pay. What are the alternatives? Instead of trying to preventing access, you can monitor access and create reports that alert management to abusers within each organization. You can have HR put more specific data security guidelines into the personnel handbook, and make it clear that violations will be punished.

## Preventing Data Leaks

As [I wrote](#) a while ago, information leak detection and data loss prevention are hot topics. Of course you want to keep your servers secured in every way, and the leading cloud vendors do a great job of protecting your data. The real data leak problem is at the end points: laptops, iPads, and smart phones that store tremendous amounts of information.

While there are solutions available to really lock down windows laptops, they almost inevitably involve special device drivers or kernel patches that can mean trouble over time. To really do the job, you'd also want to add encryption for all files to keep data from prying eyes. At least one of these solutions that explicitly works with CRM applications, but I know of nothing that works with Macs or Linux laptops.

Unfortunately, for most organizations there just isn't a solution here, other than limiting the amount of data stored on the endpoint. Security zealots will say that clumsy ILP/DLP solutions are "better than doing nothing," but the reality may be more like "the cure is worse than the disease."

## Reports that Walk

Although the law may be fuzzy about whether a salesperson's address book is his property or the company's, the law couldn't be clearer about the company's leads, contacts, deal history, and account list. Yet reps walk out the door with these all the time.

In most CRM systems, report access is basically "all or nothing." Unfortunately, management often wants the reps to be able to run ad-hoc reports to do their job while simultaneously wanting to prevent wholesale data theft.

Instead of trying to enforce a complex web of policies, it's easier to do the following:

- Make sure that the reps do not have API or Web service access to the system. The smart ones will be able to pull stuff out through Excel.
- Turn off report export privileges, if your CRM system supports this.
- Turn off their access to reporting, at least for ad-hoc stuff. If your system allows you to give reps access to canned reports only, terrific.
- Give them access to reports only through an internet "jump" page that limits which reports they see and monitors who's using what. Provide alerts to managers about employees who suddenly become excessive report users: this is often a "tell" for an employee about to leave.
- Give them access to reports only as PDFs or JPEG images — don't let them get data in exportable or screen-scrappable form.

*David Taber is the author of the new Prentice Hall book, "[Salesforce.com Secrets of Success](#)" and is the CEO of [SalesLogistix](#), a certified Salesforce.com consultancy focused on business process improvement through use of CRM systems. SalesLogistix clients are in North America, Europe, Israel, and India, and David has over 25 years experience in high tech, including 10 years at the VP level or above.*

**Follow everything from CIO.com on Twitter [@CIOonline](#).**

© 2010 CXO Media Inc.