From: www.cio.com

CRM: Avoid 3 User Identity Mistakes

– David Taber, CIO

March 22, 2011

Most of the advice in this column has been about customer data: leads, contacts, accounts, and transactions. Too often ignored is the CRM data that's about your users: employees who log in and manipulate data every day.

There are some user policies that are tempting, but have some nasty consequences. Here are three big ones we see all too often.

1. Naming Users By Their Function, Rather Than Their Name
The default login for CRM users is their name or email address. But it can be tempting to have the login be the person's function, rather than their real name.

If you have a large pool of workers that do essentially the same thing (e.g., "customer support operator 13"), this isn't the worst idea in the world. It does provide contextual information that isn't available from the user's own name, but it de-personalizes your users — never a good thing for system adoption or for HR. A better approach is to use the user's Profile, Role, or other fields to provide that information in addition to the user's name.

The bigger issue, though, is that you're tempted to try...

2. Recycling License Identities
Due to the high turnover rates in low-level sales and marketing personnel, CRM systems are much more likely to have users come and go than any other part of enterprise software. In some groups, CRM users' life span averages little more than a year.

Of course when a user is gone, you want to deactivate their license as rapidly as possible so that the license can be used by the new user. But recycling the user license is not the same thing as recycling the license identity.

In most CRM systems, the license identity (which can be thought of as a user "slot" in the system) can never be deleted: the moment it is first instantiated, records and audit trails all over the system record pointers to the slot. Indeed, in Salesforce.com, even the user name (e.g., dtaber@saleslogistix.com) can be used only once across all customer instances...forever.

It's tempting to have an administrative policy that takes that eternal slot and recycles it for a new user when the old one is gone. This avoids the clutter of slots from users who will never be on the system again. Do not fall for this temptation.

Why? Because all the system's history and audit trails will still be pointing to that slot, so that history will be falsely attributed to that new user. Six months from now, nobody will remember exactly when the new user transitioned in. If the new user has a different function in the organization, nobody will

remember what the previous user's exact role was. It's really hard to reassign accounts if you don't remember what the original user's territory was. Any historical reports will yield misleading results that cast doubt on the credibility of all the system's data. Not a good plan.

Further, recycling slots practically guarantees data quality problems over time, as people try to "fix" the data or reports to adjust for blurred user identities.

The best practice: never recycle user slots. Instead, deactivate old users and create new slots, explicitly transitioning the defunct user's data to the new owner(s) in a bulk data change.

What about the situation where a user leaves the company and comes back months or even years later? Usually, it's best to reactivate the user's old slot and transition the data that belongs to them in their new role. However, if their new role is completely different from what they were doing before (e.g., they used to be in the customer service call center, but now they're in marketing after business school) and their old identity could cause confusion in reports, using a new slot may be justified. In this case, their old avatar should be renamed (e.g., "joe.blow.OLD") to keep the identities clearly separated.

3. Sharing Licenses for Cloud Integrations

To be effective, CRM systems need to be integrated with other enterprise systems and infrastructure. That goes double for cloud-based CRM. Typically, each integration point must "log in" to the CRM system to securely share data.

If you've got several systems integrating with the CRM, it's tempting to have a policy where the systems share a single user license. Or, you might find it tempting to have each external system share logins with human users. Even if your CRM vendor's contract allows it, avoid these temptations.

The first issue here is audit trails and data forensics. If all the systems are taking action from a single login, it will be very difficult to troubleshoot bugs. In the other case, where systems are taking action while logged in as one or more users, management reports will soon become very complicated (to filter out the robot activities from the human ones) or misleading, or both.

Potentially worse is the potential for uncoordinated workloads. External system integrations operate asynchronously, and may need to update data at high speed. Having multiple integrations using the same user license may cause resource contention within the CRM system, leading to weird performance problems and bugs that can be tough to troubleshoot.

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.