From: www.cio.com

Data Loss Protection and Your CRM System

– David Taber, CIO

December 17, 2009

CRM systems are full of data that's valuable to your company. Or at least, it better be. But CRM systems are not at the top of the list for external hackers, so why should it be on your priority list for an ILP/DLP system?

Let's start by clearing up a misconception: the external hacker is rarely your biggest concern, particularly for a CRM system. The most dangerous breaches come from your own employees, particularly the disgruntled ones. Given the number of layoffs and the turnover of sales reps these days, the risk has grown. Your employees not only have access to a significant amount of data, but also know what the data means and how to separate the marginal from the important.

CRM Definition and Solutions
Unmasking DLP: the Data Security Survival Guide

So your first order of business is to prevent key CRM data from walking out the door. Legally, the data is the employer's property. But practically, your entire contact list and transaction history could fit on a microSD card that is easily hidden and transported. Although the best CRM systems have fine-grained access controls (enforced by role hierarchies, user profiles, workflow status, and application logic) and audit trails, I have yet to find one that has a meaningful level of ILP. If a user is allowed to run any reports, they can typically run almost all of them and export the results to a CSV file. If a user can see a record, they can save it as HTML or print it. And with almost every CRM vendor, there is no audit trail regarding access history.

CRM systems of course provide the ability to deny even read access, but going to that extreme both limits user productivity and tips off the bad guys that you are on to them. Instead, use a proper ILP/DLP tool.

You'll need to work closely with your ILP tool vendor, as SaaS CRM systems present some special challenges. If you haven't bought one already, make sure to look for one that is data aware, particularly in the Web context. The ILP tool will easily be configured to block creation of CSV files, or at least to prevent them from being e-mailed or downloaded. But you don't necessarily want to block the use of all CSV files, just the ones that have the contents of your CRM system. ILP tools can also be configured to block the saving or printing of an HTML page, but the very flexibility of SaaS CRM systems makes it harder to characterize the off-limits content. If this reminds you of the joys of configuring a screen-scraping tool, you're getting my point here. Salesforce.com does make things easier by using a unique URL for every object, page, and record in the system, so the ILP tool can simply be configured to key in on an entire range of pages.

Let's move on to more systemic ILP issues in CRM. Because true CRM systems are integrated with several other company data assets, you need to look at the big picture to understand your vulnerability. CRM-native data may leak out of your Accounting, Order Entry, or e-commerce systems.

CRM data may also be pushed into your customer support or warehouse/distribution software. These external systems are not likely to have the same security model as your CRM system has, so your analysts will need to look carefully for loopholes and back doors.

Of course, the reverse is also true: integration servers may push significant amounts of customer data into your CRM system from other parts of your enterprise. The highest visibility issues will relate to customer financials: social security numbers, health account numbers, bank account records, and credit card information. Although there are some good arguments for having these available in the CRM system, we always counsel our clients to avoid actually storing any sensitive customer financial data in the CRM database.

For almost any company (even in financial services), the system of record for the customer's financial data is in or near the accounting system. There's no reason to duplicate all of it in the CRM system, thereby triggering a PCI compliance audit.

A Guide to Practical PCI Compliance

Further, if you have customers in the European Union, special protections for personal and sensitive information are legally required. Instead of storing sensitive data in the CRM system, the data should be pulled over only when specifically needed to populate a screen, and be stored only in volatile memory. Data obfuscation strategies (such as fragmenting a row across several tables and linking them with hash keys) can also provide a line of defense.

Finally, you'll need to enact a series of ILP/CRM policies and procedures, such as:

• Reducing the number of people with system administrator privileges.
• Creating rules for locking down data (both for editing and access).
• Developing a policy and process for at-risk or soon-to-be-terminated employees.
• Turning off API access to the database for almost all users.
• Dramatically limiting the use of connectors to Office, Outlook, Excel, Google, or other contact managers, as well as any mass import/export tools.

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.