THE DATA QUALITY IN CRM SYSTEMS: STRATEGY AND PRIVACY

Marija Boban [1], Miodrag Ivkovic[2], Vesna Jevtic[2], Dusanka Milanov[2]
[1] *University of Split*
[2] *University of Novi Sad, Technical faculty Mihajlo Pupin Zrenjanin*

Abstract – *This work emphasizes importance of Customer Relationship Management (CRM) data for success in business, especially in marketing, sales and customer services areas. The data quality is essential for deployment of increasingly integrated operational and analytical CRM systems, as well as for meaningful set of customers' metrics maintenance. This work represents goals and strategy, factors and management program of data quality, as well as, data privacy and data security in CRM systems.*

1. INTRODUCTION

CRM data play very important role in marketing, sales and customer services areas of business and like a source of very valuable information are often treated as a business assets. When it comes to customer information, poor data quality can lead to problems that are no less important. Quality of customer data is essential for enterprises and their ability to successfully deploy and maintain increasingly integrated operational and analytical CRM systems, as well as maintain meaningful set of customers' metrics. Therefore, consistency and quality of customer data are critical components for CRM success. The CRM data stored within the CRM system include information contact details as well as other information related to people, organizations and accounts or related to records of orders and communications linked to each of these. Information that are collected by particular person or organization are accurate or true at the moment of recording. These information are prone to become inaccurate during time, and that what holds true for one moment in time may change in future. By integrating customer information from multiple touch points into one, accurate, current record, enterprises can rely on consistent segmentation to drive their treatment of customers and reveal true purchasing behaviors and patterns to forecast future sales accurately. Quality of data is subject by the following key issues:

- How can enterprises create and maintain a database of consistent, high-quality customer information?
- How can consistent, integrated customer interactions be enabled across multiple channels?
- How will enterprises evolve their analytical systems to reveal key customer insights?
- How can customer insights be profitably applied to inbound and outbound customer interactions?
- How to provide privacy for customers' information?

2. GOALS AND STRATEGY OF DATA QUALITY

This should form the introduction to the need for a data quality strategy within organization. The strategic objectives should aim to relate data to the success of organization and goals. It is often best to start by filling in a grid to identify how the results of data strategy will impact organization, as below. Common goals for CRM system are: improving communications, creating multiple touch points to serve the customer, strong relation with Enterprise Resource Planning (ERP), reduced waste of mailing budget, compliance with data regulations. Achieving the level of integrated, consistent customer data necessary to support CRM initiatives does not come easily. Most large enterprises have an average of five to ten operational sources containing customer data (see Figure 1).

Given a single, integrated view of the customer is the cornerstone of CRM, a common pitfall is to attempt to achieve this view through a single, integrated database. For all but the simplest enterprises, however, such as universal database remains elusive — held out of reach by the intricacies of multiple lines of business, geographic diversity and a legacy application mix. Therefore, most enterprise CRM implementations will be forced to use customer information sourced from multiple data stores. In this environment, identifying the most-appropriate operational sources from which customer data elements can be acquired involves significant analysis. Questions to be resolved include:

- Where data reside?
- What format they have?
- Where are duplicated data?
- Do the overlapping data have incremental value?
- Which data sources are the most reliable?

Enterprises must have three types of data to effectively manage their customer relationships: descriptive, behavioral and contextual. The interaction among these information types must be understood to provide a coherent picture of the customer relationship.

- *Descriptive data* focuses on the customer, which could be an individual, a household, a business or some combination of the three. Demographic, lifestyle and psychographic data fit into this category. Much of these data come from the enterprise's operational systems or from external data providers. It is readily available and, therefore, yields little competitive advantage.

- *Behavioral data* includes details on the transactions and interactions that comprise the relationship between the enterprise and its customers. Acquiring relationship data have proven to be the biggest challenge for many enterprises, because they must strike a balance between collecting too much and too little. These data personalize the customer/enterprise relationship.
- *Contextual data* are the least common type of information for an enterprise to have; however, an enterprise is unlikely to maintain strong customer relationships without an understanding of their context. Because contextual data are both, diverse and unstructured, it is difficult to integrate them with operational customer relationship systems.

3. FACTORS OF DATA QUALITY

Industry analysts point the finger at bad data as one of the top three reasons why CRM projects fail. Because bad data leads to misleading, incomplete, and confusing information, it lowers adoption – another major reason why CRM projects fail.

Accurate information and reports are the life blood of an effective sales force. Without it, management does not have the data to make good decisions, sales reps do not have the tools to turn leads into customers, and the company will find it difficult to reconcile CRM data with data in other systems. The results are lost opportunities and revenue, frustrated users and customers, and a lack of user adoption.

To ensure consistent high data quality, the users need to be trained, and companies need to create and implement a data quality process, and use available technologies to automate the process whenever possible. A six-step approach that is working for many companies includes as follows.

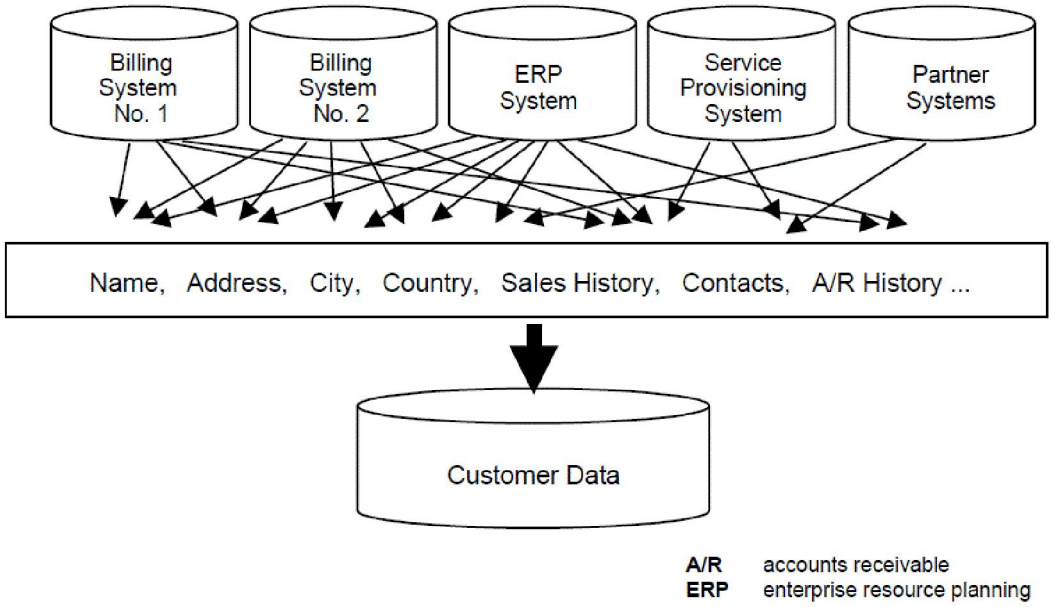

Figure 1. The Quality and Consistency Challenge in a Heterogeneous Data World [2]

3.1. Data Profile and Context

Data profiling is all about understanding data. Companies should know where their data come from: spreadsheets, backend systems, or sticky notes all over reps' desks. An inventory of the data should be taken that includes the following information:

- The data sources should be listed as well as the names of the fields in which data are stored;
- Any potential problems with the data should be noted. Companies should ask questions such as: Do we have automated quality checks before new record can be saved? Are all fields mapped correctly?

Context defines the type of data and how the data are used. Ultimately, the context of your data determines the necessary types of cleansing algorithms and functions in order to raise the level of quality.

3.2. Data Control

Data control includes achieving data accuracy and ensuring the right users have access to the right information, which also means blocking access, as needed. To control data, they should first be cleaned by removing duplicates and errors. Then, processes should be set up and technologies used to keep data clean. Some guidelines can be outlined as follows:

- Use automated routines or tools to clean your data;
- Prioritize your data cleanup effort. First fix data which are highly visibly and frequently used, such as addresses and emails. Fix business-specific information next, such as opportunity types and

stages. Finally, remove any duplicated fields; for example, do not repeat account information in the contact object;

- Get your users to fix their data. You can alert users when data records are incomplete or do not conform to data-quality standards;
- Use exception reports and data-quality dashboards to remind users when their accounts and contacts are incorrect or incomplete. Scheduling a dashboard refresh and sending that information to managers is a great way to encourage compliance;
- Review your profiles and role hierarchy and make sure the hierarchy, teams, and groups are kept up to date;
- Meet frequently with management to keep up with organizational changes;
- Define the Create, Read, Update, and Delete (CRUD) rights for each profile to ensure users can work with data, as needed.

3.3. Integrate data and storage

Most organizations have data in more than one system. Whenever there are duplicated data in several systems, it is easy for information to get out of synch. One way to avoid this problem is to integrate systems so that updates in one system automatically update the others, resulting in a single source of "truth" and making it easier for end users to access information. When designing the integration, company should evaluate their business applications to determine which one will serve as system of record for the synchronization process. The system of record (or master) can be a different system for different business processes.

Every data quality strategy must consider where data physically reside. Considering storage as a data quality factor ensures the physical storage medium is included in the overall strategy. System architecture issues – such as whether data is distributed or centralized, homogenous or heterogeneous – are important. If the data reside in an enterprise application, the type of application (CRM, ERP, and so on), vendor, and platform will dictate connectivity options to the data.

3.4. Augment data

To make a CRM system even more valuable, the data should be augmented with information that will give the salespeople and managers an edge. For example, companies should make the most of internal market intelligence, such as purchasing patterns or competitive analyses. To understand what kind of data are valuable, they should survey the sales and marketing users to see what they want the most. Also, an internal information about customers' behavior and buying patterns should be collected and then evaluated, if it is helpful.

3.5. Monitor data

Achieving high-quality data is not a one-shot effort, but requires ongoing vigilance. Establishing policies, processes, and tools for monitoring data is crucial to maintaining data quality. A centralized process for mass data loads and data-cleansing projects should be defined.

3.6. Assign ownership, train users and commit to a data-quality process

Users need to know the importance of data integrity and how to do their part in any data-quality initiative. During users training, companies should show them how data quality directly affects their work. It's also a good idea to assign ultimate responsibility for each region's data to a super user, geographic lead, or other business owner.

4. CUSTOMER DATA QUALITY MANAGEMENT PROGRAM

Best practitioners of Customer Data Quality (CDQ) management program combine vision, technology, culture and business rules to cultivate more intimate and relevant relationships with their customers.

Establishing a successful CDQ program requires more than just applying the right data quality software to the problem. It is imperative that organizations first identify and resolve any underlying business or cultural issues impeding customer information management. Prioritizing objectives to be achieved with the CDQ program is the next order of business.

When those fundamental matters have been adequately addressed, an organization can confidently embark upon the implementation of a CDQ program, which is comprised of the following components:

- Discovery & Analysis
- Data Conversion & Cleansing
- Data Quality Maintenance
- CDQ in Enterprise-wide CRM
- Legality & privacy

Best practitioners of CDQ will not stop once they have completed the initial data analysis, data conversion and data cleansing. Ongoing data quality processing is necessary to maintaining the integrity of any CRM system. Changes are constantly being made and new data is always being introduced into the system from various sales channels, including and especially the Web.

The Web presents a special challenge to data quality maintenance because the responsibility for data input lies more with the e-customer and less with the organization. Organizations that value their customer information will place a data quality filter at all customer interaction touch points, including the Web. This filter is the organization's defense against customer data corruption. After the CRM system is populated with cleansed and linked data, organizations will want to focus their preventative data quality measures on the front-line, rather than on more costly and time-intensive back-office clean-up. Just as business rules were critical to the conversion, data quality filters must be flexible and robust enough to support the organization's established business rules. This consistency will ensure the organization's data quality conversion efforts are maintained going forward.

5. DATA PRIVACY IN CRM SYSTEMS

The right to data privacy is heavily regulated and rigidly enforced in Europe. The European Court of Human Rights has given this article a very broad interpretation in

its jurisprudence. According to the Court's case law the collection of information by officials of the state about an individual without his consent always falls within the scope or article eight. Thus, gathering information for the official census, recording fingerprints and photographs in a police register, collecting medical data or details of personal expenditures and implementing a system of personal identification have been judged to raise data privacy issues.

Any state interference with a person's privacy is only acceptable for the Court if three conditions are fulfilled:

1. the interference is in accordance with the law,
2. pursues a legitimate goal and
3. is necessary in a democratic society.

Private companies are engaged in threatening activities, especially since the automated processing of data in CRM systems became widespread. As the entire member states of the European Union are also signatories of the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Commission was concerned that diverging data protection legislation would emerge and impede the free flow of data within the EU zone.

Therefore the European Commission decided to harmonize data protection regulation and proposed the Directive on the protection of personal data. In full name, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice. The personal data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept longer than necessary;
6. Processed in accordance with the data subject's rights;
7. Secure;
8. Not transferred to countries without adequate protection

The directive regulates the processing of personal data, regardless if the processing is automated or not. Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a). This definition is meant to be very broad. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data": address, credit card number, bank statements, criminal record.

The notion processing means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (art. 2 b)

The responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d)

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any on line shop trading with EU citizens will process some personal data and is using equipment in the EU to process the data (the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules. The directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject. That is why all of the EU countries have developed their own legislative in data protection on the traque of these directives.[1]

In contrast European state-to-state approach, Canada has, through Personal Information Protection and Electronic Documents Act - PIPEDA[2], chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. Organizations not governed by PIPEDA for commercial activities within a province need to be aware that PIPEDA applies to transborder transfers. However, under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The OPC can investigate complaints and audit the personal information handling practices of organizations.

---

[1] For example, in Croatia, the protection of personal data is regulated since 2003. by the Law on protection of personal data, as well as the Law of the right to data privacy. On the traque of European directives, as the crown of this process, information security is regulated and enforced since 2007. by the Law on information security. In Serbia the Law on protection of personal data is also issued in the year 2010. also on the traque of the European Directives.

[2] The Office of the Privacy Commissioner of Canada (OPC) has developed these guidelines to explain how the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to transfers of personal information to a third party, including a third party operating outside of Canada, for processing. The guidelines do not cover transfers of personal information for processing by federal, provincial or territorial public sector entities. Nor do these guidelines deal with any specific rules governing transfers for processing that may be found in provincial private sector privacy laws. For more information look at ◦Federal Privacy Commissioner – Guidelines for Processing Personal Data Across Borders, http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf , 08. 02. 2011.

6. INFORMATION SECURITY MANAGEMENT SYSTEM AND THE CREATION OF SECURITY POLICIES IN CRM SYSTEMS

Evidently, in modern digital economy, information is the lifeblood of business and organisations are increasingly dependent on the use of information systems and networks to process information. Computer 'literacy' is now widespread making systems ever more open to abuse, whether deliberate or accidental. Consequently, businesses are increasingly at risk through use of the very tool introduced to increase efficiency, i.e. information technology (IT). Managers must therefore address these risks where they would affect their systems and the information used on them in terms of:

- confidentiality
- integrity
- availability.

as it is shown on the Figure 2[10].

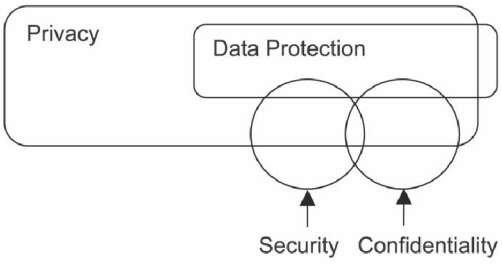

Figure 2. Basics of Information Security Management System

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results. If managing an organization's information security risks quality, the most important is to choose the best methodology. The model of Risk management is presented at the Figure 3 [11].

In the increasingly interconnected business environment, information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Information can exist in many forms: it can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. It is important to stress that information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

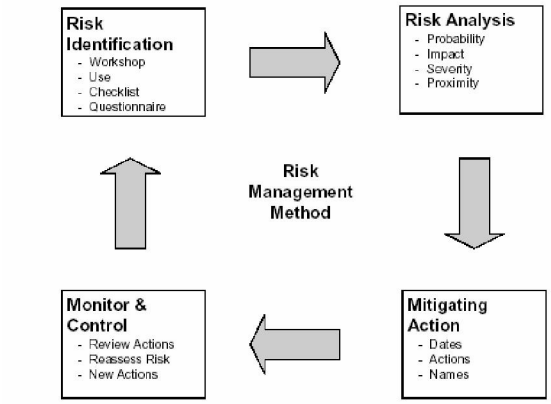

Figure 3. Model of Risk Management Method

In organisation environment, information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

Information security policy[3] in accordance with the application of ISO 27001:2005[4] 4.2.1 b must be defined as follows:

"The organization must do the following:"

- Define the scope and limits of ISMS in terms of business features, organization, its location, assets and technology including details and justification of any exclusions from the scope
- Define the ISMS policy in terms of features, business, organization, its location, assets and technology that:
  - includes a framework for setting goals and establishing overall sense of direction and principles for acting in relation to information security,
  - takes into account the business and legal or regulatory requirements and contractual obligations related to security,

[3] General security policy is binding for the entire organization. With defining of a specific security policies, general security policy is specified and descends to the lower operational levels. Specific security policies regulate individual aspects of business processes that wish to be maintained under control of ISMS. The area for which are defined the specific security policy must be within the scope of the ISMS and the policy must be consistent with the general policy of the ISMS.

[4] ISO/IEC 27001:2005 - Information technology - Security techniques -- Information security management systems - Requirements

- it is consistent with the organizational context of strategic risk management within which will be made the establishment and maintenance of ISMS;
- establishes the criteria by which risks will be evaluated (see 4.2.1c)), and
- is approved by management.

And according to the requirements of Annex A:

A.5.1 Information security policy – the goal: "Provide guidance and support from management for information security in accordance with business requirements and applicable laws and regulations.

A.5.1.1 Information security policy document must be approved by management, must be published and all employees and relevant external parties must be familiar with it.

A.5.1.2 "Information security policy must be viewed at planned intervals or if significant changes to ensure the lasting relevance and effectiveness.

6. CONCLUSION

As it is shown, consistency and quality of CRM data are crucial for business success. In order to prevent incorectness of data, enterprises develop strategy and goals of data quality. Enterprises use descriptive, behavioral and contextual data types to effectively manage their customer relationships.

Factors which ensure consistent high data quality are represented by six-step approach including: data profile and context, data control, data integration and storage, data augmentation, data monitoring, assigning ownership, users training and commitment to data-quality process.

Important issues of CRM systems are data privacy and information security policies. Data privacy is very delicate issue and every EU country has developed its own legislative in data protection. Information security in organisation environment is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls are part of information security management system which ensures accomplishment of specific security and business objectives of the organization.

ACKNOWLEDGMENT

This research is supported by Ministry of Science and Technological Development, Republic of Serbia, under the project number TR32044 “The development of software tools for business process analysis and improvement”.

7. REFERENCES

1. George Fratian, Planning your CRM SAP Implementation, Galileo Press, 2008
2. CRM Data Strategies: The Critical Role of Quality Customer Information, Gartner, Executive Report Series, 2003
3. Russ Lomabrdo, CRM for the Common Man, PEAK Sales Consulting, LV, USA, 2006
4. Jill Dyche, CRM Handbook A Business Guide For CRM Customers, Addison Wesley IT Series, 2004.
5. http://www.destinationcrm.com/Articles/
7. http://knol.google.com/k/crm-data
8. http://trilliumsoftware.com/home/solutions/enterprise
9. http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf
10. www.cihi.ca/partship/conoct99/peladeau.pdf
11. Wilhen Associates Limited/ Project Frameworks Solutions Limited October 2002.