2005

Risk management in CRM security management

Mahdi Seify

Risk Management in CRM Security Management

Mahdi Seify
Sharif University of Technology-Faculty of Industrial Engineering-Tehran-Iran
Mahdiseify@yahoo.com

Abstract

In an increasing competitive world, marketing survival can be depended simply on timely new information on customers and market trend. One of the most important strategies in CRM (Customer Relationship Management) is to capture enough information from customers and using this information carefully [Ryals , Tinsley]. Of course security of this information is very important in CRM data management [Bryan]. Data management is a method for scheduling and controlling data saving, recovering and processing. This activity has been done continually or periodically[Bryan]. Security level of this information depends on the security policy of the organization. CRM security policy is the directives and practices for managing, protecting and distributing assets which are included sensitive information, within an organization and its CRM systems[ISO/IEC TR 13335, ISO/IEC 17799, and BS7799]. CRM security policy is a high level plan that focuses on the strategic security methodology and is not limited to the guideline, standard or control way and plays a critical role in the defense of CRM systems and network [Barman, M.Amanda]. CRM risk evaluation is a method for increasing the efficiency of CRM security policy. In the manner that security threats and vulnerabilities against CRM is identified by its priority [Greenstein, Bryan, and ISO/IEC TR 13335]. First of all in this article, the importance of risk management in CRM is found out and then the suggested method of security risk management is introduced.

Keywords

Risk Management, Customer Relationship Management (CRM), Data management, Information Security Management System (ISMS).

INTRODUCTION

There is a major change in the way of companies which can organize themselves as they switch from product based to customer-based structures. Start of this change is the advent of CRM which converges information systems and develops supporting software. CRM significantly causes to improve the implementation of relationship marketing principles.

CRM has different meanings, It is a business strategy to select and manage customer to optimize long-term value, CRM also is a strategy that increases the importance of relationship marketing and integrates with other organization strategies [Ryals, Tinsley].

Implementing CRM requires a customer business philosophy and culture to support effective marketing, sales and service processes. Amounts of sophisticated software from companies such as Siebel, Oracle and Nortel Networks are growing [Tinsley].

Despite the efforts of CRM on efficiency and affectivity of management decisions, statistics reflect that unreasonable decisions are made by CRM systems; IT experts said “errors were caused by incorrect or not enough data” [Bryan, Stanley]. For making hard decisions CRM needs data management system [Felix, Bryan]. Data management helps to capture exact, qualified and up-to-date information about market, company, competitors and etc. On the other hand, according to my experiences and other experts words, security management system is very important to have a dramatic increasing in the performance of data management [Bryan]. My suggested method to

manage CRM risk is based on the establishment of Information Security Management System (ISMS) for CRM Data Management.

In this paper has tried briefly to introduce suggested method for risk management in CRM Security Management System.

DATA MANAGEMENT IN CRM

Data quality has always posed problems. Incorrect or incomplete data leads to internal frustrations and inaccurate marketing. Despite spending considerable sums of money on CRM software, most of them state that there have been few major improvements to the quality of customer data in the past few years. My research shows that the most of the CRM managers need to increase significant improvement in the quality of data management.

Establishing and implementing data management are an important part of increasing quality of CRM data. Of course, more effort on data management method causes a sharp rise in short term and long term benefits and extends market.

Data management ensures that the organization [Bryan, Stanley]:

- Has data flows control into and out of the business;
- Knows what data is collected and why; where, it is held;
- Knows how the data is used in the organization, and by whom;
- Knows what value the data brings to its business processes.

Recently, many companies have made significant investment in E-business initiatives. The first step was to ensure that in their new E-business their operational systems met financial requirements and performed to acceptable standards. Many companies had to re-engineer their resources for improving security, increasing scale of systems so they were accessed by over-larger and more unpredictable flows of customers. With these achieved objectives, many companies are now focusing on using their systems to manage customers for increasing profitability.

A number of issues arise in the area of the data management [Bryan, M.Amanda, and Stanley]:

- **Data capture**: understanding what data needs to be captured and at what stage in the relationship, in what way and how frequently.
- **Data systems**: reviewing the needs for changing to data systems to manage e-business.
- **Data quality and maintenance**: understanding the way the data is held, knowing what you have and how good it is.
- **Data analysis**: enriching exiting data and identifying how to make the most out of it. In an E-business environment, the extent of the data that can be analyzed includes not only the standard details about customers, but also the ways in which those customers use the E-business channels.
- **Data security**: including data privacy and fraud.

According to the role of data management in CRM, and also significant role of CRM in E-commerce, the importance of security in CRM is approved [Greenstein, Stanley, and M.Amanda].

Confidentiality and security on World Wide Web is low; in consequence, there is no assurance on CRM analysis if CRM Security Management System has not been used.

In the next part of this paper, I point to suggested method on CRM Security Management System.

CRM SECURITY MANAGEMENT SYSTEM

There is an increasing international focus on data protection and privacy in the communication age. World-companies need to be ensured that individuals' rights and information are adequately protected. As different

countries have taken different stances, it is caused an inconsistent set of rules, there is an increasing pressure to work together to protect the rights of consumers as personal information crosses international broader.

During recent years, Government and commercial organizations rely heavily on the use of information to conduct their business activities. The loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and services can have adverse impacts on organization [ISO/IEC TR 13335, ISO/IEC 17799, and BS7799]. On the one hand, fall in to habit of using CRM system in all levels of organization, being worried for security of information; On the other hand, IT administrators must monitor security on huge and complex computer networks.

This requirement to protect information is particularly important in today's environment because many organizations are internally and externally connected by networks of IT systems. This problem has been causes to establish a new professional science about security management in CRM for implementing ISMS [TSSIT, ISO/IEC TR 13335, ISO/IEC 17799, and BS7799]. That is named CRM Security Management System (CRM-SMS) by me.

A CRM-SMS process can be used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability in relationship marketing. The management of CRM security includes the analysis for the security requirements, the establishment of a plan for satisfying these requirements, the implementation of this plan and maintenance and administration of the implemented security. According to current standards and CRM systems, six steps are suggested for CRM-SMS implementation [Felix, Bryan, Stanley, and ISO/IEC TR 13335]. A brief summary of each risk management paradigm activity follows:

1. Determining organizational CRM security objectives, strategies, and policies.
2. Identifying and analyzing the security threats to, and vulnerabilities of the assets of CRM systems within the organization.
3. Implementing CRM security plan
4. Developing and implementing CRM security awareness and training program
5. Following up the CRM security plan.

Determining organizational CRM security objectives, strategies, and policies

the first step in the process of managing CRM security is to consider on this question" which broad level of risk is acceptable to the CRM system?" The necessary broad level of security is determined by the CRM security objectives which an organization needs to meet.

Depended on the security objectives, a strategy should be agreed upon. A CRM security strategy outlines in general terms how an organization will achieve its CRM security objectives.

After establishing the organization's CRM security objectives and CRM security strategy we should form a basis for the development of a corporate CRM security policy. The development of a corporate CRM security policy is essential to ensure that the results of the risk management process are appropriate and effective. Management support across the organization is required for the development and effective implementation of the policy. This policy and these standards define the minimum requirements to which each State agency, including employees and contractors, must adhere. The primary objectives of the CRM Security Policy are:

- To establish a secure environment for processing customers data
- To reduce information security risk
- To communicate the responsibilities for the protection of information. It is essential that a corporate CRM security policy considers on the corporate objectives and particular aspects of the organization.

Identifying and analyzing the security threats to, and vulnerabilities of the assets of CRM systems within the organization.

The object of this step is to identify and assess the risks to which the CRM systems and its assets are exposed, in order to identify and select appropriate and justified security safeguard. The likelihood occurred threats lead to the potential adverse business impacts.

Implementing CRM security plan

The CRM security plan is a co-ordination document defining the actions to be undertaken to implement the required safeguards for a CRM system. This plan should contain the results of the review described above, the actions to be undertaken within short, medium and long time frames to achieve and maintain the appropriate security level, the costs, and an implementation schedule.

For the implementation of safeguards, all the necessary steps are described in the CRM security plan should be carried out. The responsible person for the plan (which normally is the CRM system security officer) should ensure that the priorities and the schedule outlined in the CRM security plan are followed.

Developing and implementing CRM security awareness and training program.

The objective of the security awareness program is to increase the level of awareness within the organization to the point where security becomes second nature and the process becomes a routine that all employees can easily follow.

Besides the general security awareness program, which should apply to everybody within an organization, specific security training is required for personnel with tasks and responsibilities related to CRM security. The degree of depth of security training should be depended on the overall importance CRM security has for the organization, and should vary according to the security requirements of the performed roles.

Following up the CRM security plan

Follow-up, even though often neglected, is one of the most important aspects of CRM security. The results of follow-up actions are such as security compliance checking of implemented safeguards, monitoring and reviewing CRM security in day-to-day use, and reports of security relevant incidents. The implemented safeguards can only work effectively if they are checked in real business life. It must be assured that they are used correctly, and that any security incidents and changes are detected and dealt with:

1. Following up the CRM Incident Handling and disaster recovery
2. Following up the CRM security monitoring and maintenance
3. Following up the CRM security change management
4. Follow up the CRM-SMS Compliance

Following up the CRM Incident Handling and disaster recovery*:*

To identify the risks and to measure their severity it has been emphasized that risk analysis is required. To support risk analysis and enhance the results, information is required on security incidents. This information has to be gathered and analyzed in a secure way, and be seen to provide benefit. Thus it is important that any organization has a properly constructed and organized CRM Incident Analysis Scheme (CRM-IAS) in operation, and that the information received and processed should be available to support risk analysis and management and other security related activities.

Following up the CRM security monitoring and maintenance*:*

Monitoring is an ongoing activity which checks the system, its users, and the environment maintain the level of security as laid out by the CRM security plan. A plan for day to day monitoring should be prepared to provide additional guidance and procedures for ensuring ongoing secure operation.

Following up the CRM security change management:

CRM systems and the environment in which they operate are constantly changing. These changes are a result of the availability of new features and services, or the discovery of new threats and vulnerabilities. These changes can also result in new threats and vulnerabilities. Change of the CRM system includes:

- New procedures
- New customer behavior and needs
- New features
- Software updates
- New CRM technology
- New users to include external groups or anonymous groups, and
- Additional networking and interconnection.

When a change to a CRM system occurs or is planned, it is important to determine what, if any, impact the change will have on the security of the system. If the system has a configuration control board or other organizational structure to manage technical system changes, the CRM system security officer, or his/her representative, should be assigned to the board and be given responsibility to make determinations about whether any change will impact security, and if so how.

Follow up the CRM-SMS Compliance:

Security compliance checking is the review and analysis of the implemented safeguards. It is used to check CRM systems or services to the security requirements documented in the CRM systems or services conform to the security requirements documented in the CRM system security policy and CRM system security plan.

The head of each agency is responsible for compliance with and enforcement of this Policy. Agency Chief Information Officers (CIO) shall develop and implement an Agency CRM Security Program to implement this policy and these standards. The Security Program shall include a timetable and controls for compliance. The controls shall include the following items but are not limited to these ones:

- Maintaining the confidentiality, integrity, availability, and accountability of all States of CRM applications and services.
- Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed
- Ensuring that risks to information security are identified and also controls these risks.
- Implementing processes to ensure that all security services meet the minimum requirements set force in this policy and the attached standards.
- Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations
- Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's CRM assets

According to above statements, important parts of the CRM-SMS are the assessment of risks, and how they can be reduced to an acceptable level. After assessing the security requirements of the CRM systems and services, it is advisable to select a corporate risk analysis strategy. Following the risk assessment, appropriate safeguards are identified for each CRM system to reduce the risks to an acceptable level. These safeguards are implemented as outlined training program, which is important for the effectiveness of the safeguards.

RISK MANAGEMENT IN CRM

Any organization that wants to enhance security should put in place a strategy for risk management that is suitable for its environment (customers and organization,), and contains the means to address the risks in effective manner. A required strategy focuses on security effort where it is necessary and enables a cost and time effective approach [Wateridge, Finne].

If an organization decides to do nothing about CRM security, or to postpone the implementation of safeguards, management should be aware of the possible implications of this decision, by risk assessment report.

This risk assessment during the acquisition planning phase is a critical step. It is used to determine what types of controls will be cost effective and will form the basis for determining mandatory and desirable specifications. The analysis, like other risk analyses, should consider assets, threats to the assets, potential vulnerabilities, and what can be done to reduce risks. This risk assessment should take into consideration existing controls and their effectiveness. This risk assessment will require participation by the other functional groups. This risk assessment will use input from the analysis of integrity, availability, and confidentiality requirements as the basis for determining the value of customers and market information assets and the impact of security failures. The selection of appropriate types of safeguards should take into consideration the results of the level of assurance analysis [ISO/IEC 15408].

Risk management has been affected on CRM life cycle. Threats and vulnerabilities of CRM system data is completely recognized and solved by suggested method. At last briefly suggested method which has following eight steps is proposed [Bryan, Greenstein, ISO/IEC TR 13335, ISO/IEC 17799 , and BS7799]:

Step1: Information Gathering

The aim of this module is to collect all the important information in the following assessments. Prior to gathering input for the CRM asset identification and valuation, the boundaries of the review should be defined. A careful definition of boundaries at this stage avoids unnecessary work and improves the quality of the risk analysis. This module contains the steps:

Step1-1: Definition of the CRM- Security Management System (CRM-SMS)

The name of the company and scope of the review are based on CRM security policy, interfaces and dependencies are identified.

Step1-2: Asset Identification

All assets in the CRM-SMS are identified like customer information, CRM services, CRM document, CRM arrangement and procedures, CRM software and programs, CRM hardware, CRM media, connections and communications, building and equipment, personnel and organization and reputation.

Step1-3: Asset Valuation

Those wishing to carry out a detailed risk assessment can identify values for the confidentiality, integrity and availability of the CRM assets. In addition, another valuation criterion can be identified for each CRM asset. The valuation scale is low, medium or high.

Step2: Gap Analysis

The Gap Analysis allows checking of the security status of the CRM against the reasonable standard like as BS 7799, ISO/IEC TR 13335, ISO/IEC 17799 and TSSIT controls.

Step3: Identification of Security Requirements is based on CRM security policy and gap analysis report.

This module concentrates on the identification of security requirements resulting from threats and vulnerabilities, and legal and business requirements. The three steps in this module are:

Step3-1: Identification of Threats and Vulnerabilities

A threat has the potential to harm the CRM system. Threats may be of natural or human origin, and could be accidental or deliberate; and on the other hand, vulnerabilities includes identifying weaknesses in the physical environment, organization procedures, personnel, management, administration, hardware, software, or communications equipment that may be exploited by a threat source to cause harm to the assets.

The threats and vulnerabilities applicable for the CRM assets are identified like as security breaches, breaches of legislation, incidents, misuse, unauthorized access, unauthorized changes, malicious code, processing errors, threats to information exchange, threat related to cryptography, user's errors, threat to mobile computing/teleworking, physical threats and disaster and interruptions.

Step3-2: Identification of Legal and Contractual Obligations

The legal and contractual obligations applicable for the CRM assets are identified like compliance with governing and marketing laws, data protection and privacy of customer information, intellectual property rights (IPR) and CRM software copyright, Outsourcing contract, right of audit in third party contracts, sub contractual obligations and assignment, regulation of cryptography controls, evidence in connection with litigation, prevention of misuse of information processing facilities and safeguard of CRM system and organizational records.

Step3-3: Identification of Business Requirements

The business requirements applicable for the CRM assets are identified, like co-ordination of security actives, compliance with standards, compliance with CRM security policy, confidence by key institution, correct business processing, maintenance by competitiveness, out sourcing and use of third party contractors, secure electronic commerce, secure internet, secure intranet, secure mobile business, secure teleworking, timely deliveries to customers and clients and timely start of new ventures.

Step4: Decision for Baseline or Detailed Risk Assessment

In this module, a decision is made on which form of risk assessment (baseline or detailed risk assessment) is suitable for which CRM assets identified for the CRM-SMS Valuation of assets and establishment of dependencies between CRM assets

Step5: Baseline Assessment

An organization could apply baseline security to CRM system by selecting standard safeguards. Identification surfaces risks before they become problems and adversely affect a project.

In detail, the steps in this module are:

Step 5.1: Controls for CRM Threats and Vulnerabilities
Step 5.2: Controls for CRM Legal and Contractual Obligations
Step 5.3: Controls for CRM Business Requirements

After fulfilling the objective of asset identification by listing all assets of the CRM system under review, values should be assigned to these assets.

Step6: Detailed Risk Assessment

Accounting and analyzing the risk of related CRM threats and vulnerabilities. The results from these activities are used to assess the risks and after that security safeguards are identified.

In detail, the steps in this module are:

Step 6.1: Valuation of Threats and Vulnerabilities
Step 6.2: Valuation of Legal and Contractual Obligations
Step 6.3: Valuation of Business Requirements
Step 6.4: Risk Calculation
Step 6.5: Identification of Controls for Risk Reduction

Step7: Selection of Controls

The measures of determined risks in the previous step should be used for identifying all safeguards that are necessary for appropriate protection.

In detail, the steps in this module are:
Step 7.1: Refinement of Selection
Step 7.2: Implementation of Selected Controls

Step8: Reviewing and reforming CRM security policy and strategy.

The policy should be maintained and reviewed according to a defined review process base on risk analysis report.

CONCLUSION

In 21 century and competitive world, suggested method for CRM Security Management System (is named CRM-SMS) can play a critical role to increase confidentiality, integrity, availability, accountability, authenticity and reliability of CRM information and services; on the other hand, Risk Management has important role in CRM-SMS and it has 8 steps. The steps in my suggested methodology are:

Step1: Information Gathering

Step2: Gap Analysis

Step3: Identification of Security Requirements base on CRM security policy and gap analysis report.

Step4: Decision for Baseline or Detailed Risk Assessment

Step5: Baseline Assessment

Step6: Detailed Risk Assessment

Step7: Selection of Controls

Step8: Reviewing and reforming CRM security policy and strategy.

RESOURCES

Barman, S. (2001) “Writing Information Security Policies”, New Riders.

Bryan, F. and Merlin, S. (2002) " CRM in financial services”, Kogan page.

BS7799 (1998) ”Information Security Management.part2: Specification for information security management systems”.

Felix, T. (2002) “Global Perspective of Information Technology Management”, IRM Press.

Finne, T. (2000) "Information Systems Risk Management: Key Concepts and Business Processes", PricewaterhouseCoopers, P.O.Box 1015, FIN-00101, Helsinki, Finland.

Greenstein and Feinman (2000) “Electronic Commerce”, Tata McGraw-Hill.

Handbook for Computer Security Incident Response teams (1998), CMU/SEI.

ISO/IEC TR 13335-1 (1996) “Information Technology –Guidelines for the management of IT security .Part1 concepts and models for IT security”.

ISO/IEC TR 13335-2 (1997) “Information Technology –Guidelines for the management of IT security .Part2 managing and planning IT security”.

ISO/IEC TR 13335-3 (1998) “Information Technology –Guidelines for the management of IT security .Part3: Techniques for the management of IT security”.

ISO/IEC TR 13335-4 (2000) “Information Technology –Guidelines for the management of IT security .Part4: Selection of safeguards”.

ISO/IEC 15408-1 (1999)”information Technology –security technology-evaluation criteria for IT security part1: Introduction and general model”.

ISO/IEC 15408-2 (1999)”Information technology-security technology-Evaluation criteria for IT security part2: Security function requirements”.

ISO/IEC 15408-3 (1999)”Information technology-security technology-Evaluation criteria for IT security part3: Security assurance requirement”.

ISO/IEC 17799 (2000) ”Information technology-code of practice for information Security Management”.

M.Amanda, Andress (2000) “getting to know your needs and putting security policies in place”.

Ryals, L. and Knox, S. (2001) "Cross-Functional Issues in the Implementation of Relationship Marketing Through Customer Relationship Management", Cranfield University School of Management.

Stanley B. (2000), “Customer Relationship Management”, John Wiley & Sons Canada Ltd.

Tinsley, Dillard B. (2002) "Relationship marketing’s strategic array", Stephen F. Austin State University, Nacogdoches, Texas.

Technical Security Standard for Information Technology (TSSIT), (1997).

Wateridge, J. (1999) " The role of configuration management in the development and management of Information Systems/Technology (IS/IT) projects " , Bournemouth University, The Business School, Bournemouth University, Fern Barrow, Poole, Dorset BH12 5BB, UK.

COPYRIGHT