Information security risks in a customer service call center infrastructure. Guidelines for security managers

Manuel Tupia
Pontificia Universidad Católica del Perú
Avenida Universitaria 1801
San Miguel, Lima 32, Perú

Abstract- IT risk management is the fundamental basis for the decision – making process relating to the implementation and use of technology initiatives at the organizations, especially for telecommunications companies. Those companies provide support services to the customers by call – centers, they are exposed to Government regulations and they have IT Risk from their infrastructure. This paper presents guidelines for security manager to establish treatment alternatives.

I. INTRODUCTION

The rise of enterprise communications worldwide, has carried them extend their technical and customer services through different channels. The main diatribe that face customer managers is to automate fully or partially those services. Some initiatives had used IVR technology (Interactive voice response) [1]. By the other side, others are keeping the customer attention with a human agent of the “other side of the phone”.

To use human agents combined with information systems, the call center are exposing to a number of IT risks ranging from human failures to software faults which would cause discontent on the client and damage to the image of the telecommunications companies.

This article briefly introduces some risks related to the use and operation of information systems in call center with human agents as well as the security guidelines useful for security managers.

II. SCOPE AND CHARACTERISTICS OF INFORMATION SECURITY ON CALL CENTER INFRASTRUCTURE

A. Characteristics of information security

A security manager or CSO (chief security officer) must guarantee confidentiality, availability, integrity, auditability and non-reject for all information residents in organization’s systems. The call center infrastructure (or simply call center) has specific risk which attempt against those five characteristics. The IT Risks have two perspectives without being excluding:

1) Risks caused by human beings [2]: using information systems (IS) on call center platforms. We can list human failures, sabotage, fraud and accidental idiot.

2) Risk caused by software and hardware involved [3]: call pooling failures, KPI (key performance indicators) erroneous, hardware failures, customer data base failures and ambient risks.

B. Information security risk treatment

Each one requires a special risk management plan according to the organization’s risk appetite with the four treatment alternatives: eliminate, mitigation, acceptance and transference [4], [5].

1) Risk caused by human intervention: The main focal point of risks of any type of IT is the human being who uses it. And the main reason of this danger is the ignorance of his responsibilities and the function’s scope over the IS, aside from cybercrimes or frauds committed conscientiously [6].

The main treatment alternative here is clear: training and awareness (to the employees) to mitigate associated risks. The second alternative treatment for the acceptance of risks is the segregation of functions, which implies that each employee knows the implications of their use of call center infrastructure and the current failures. Both programs are responsible for the areas of human resources, legal, and systems area.

2) Risk caused by software or hardware: Call center infrastructures area complex [MSS03]. Normally they include: user terminals, data servers, application servers, mixer servers for attention and pooling of the incoming telephone calls. More common risk are: software failures (errors at the time of attend incoming calls), hardware failures, inadequate maintenance process failures (with or without outsourcing), environmental failures in the server room (temperature, humidity, smoke control, security signs), absence of business continuity plans and disaster recovery plans, error in the emission of KPIs for regulatory compliance, etc. The possible options are mitigating or transferring the risk [7]:

- Mitigate the risk of software failures with appropriate application controls, monitoring activities and internal or external audits.
- Mitigate the risk of hardware failures setting replacement and contingency plans. Or set up quality assurance contracts with third-parties in the case of an outsourcing of the maintenance functions, transferring the risk.
A. Training and awareness plans

The principal focus of threats for information security is the employees of the same organizations, who by their dissatisfaction or ignorance can damage large and costly information and business continuity [11].

Non-technical solutions will be effective until to train users on their responsibilities about information security and they understand the need to integrate these concepts into their daily work.

Agents operating in Call Centers should be aware that manage the organization's vital information: on one size to have data on the attention customers, which are inputs for business indicators. On the other hand they handle personal information of customers who use the service and therefore demand the greatest of care.

Awareness and training plans should be organized by the areas of Human Resources, IT, security, and event legal area.

B. Considerations of security before, during and after labors relations

ISO/IEC 27001: 2005 divided clearly the employment relationship in these three stages (before, during and after) along with the controls security should be.

Before the employment process it is recommended to the CSO documenting the roles and responsibilities relating to safety and associated with each job, investigate the (police, judicial) background of the candidates and make them know the terms and conditions of their employment.

During employment, the CSO should remember the responsibilities for direction positions, training programs should be taken by each employer, and it must spread towards the employees the current disciplinary processes associate for faults on information security responsibilities.

Finally, at the cessation of work, the CSO must be worry by the return of assets that were assigned to the employee and the withdrawal of their rights of access to information assets.

C. Segregation of functions

ISACA [12] presents the need to realize functions segregation of jobs (charge per charge) as a dissuasive measure of crime. It is necessary to Senior Management to set the appropriate organizational structure to avoid overlaps. Both the Information Security Committee and the CSO can regularly assess the organizational structure to verify their effectiveness. In the specific case of Call Center operators, those don’t have to manipulate information of the goals indicators and simultaneously of taking care of the clients..

D. Recovery plans of hardware failures

Even if they are IVR solutions, the Call Centers have special hardware for mixing the phone calls. They could have voice responses generation cards. On these cases, their servers manage software to register the data of the attentions, the same data of the clients and offered services and the indicators of management for compliance goals [13].

Requires that the CSO has a detailed to the different types of fault recovery plan: processors, calls mixer, hard drives, RAM memories, supply of electricity, etc. This situation is particularly difficult when intervening third parties in the supply of parts and equipment, both maintenance and replacement. Even outsourcing contracts should be reviewed to verify for replacement parts and equipment since often times replenishment and spare computers similarity is not appropriate (e.g. replace a computer by another "substantially equivalent").

E. Considerations on business continuity and disaster recovery.

Disaster recovery or business continuity plans and programs provide for the resumption of all IT critical functions into the organization. Another solution that isn't viable for Call Centers the maintaining service for relevant telecommunications companies’ regulation issues. The type of solution "hot site", involves other vendor to provide service customer once produced the disaster. It is common in this type of business strategy is to have their Call Centers in different countries for economic purposes and continuity

ACKNOWLEDGMENT

We thank to CONSORCIO ECUATORIANO DE TELECOMUNICACIONES – TELCEL for support in the preparation of this article.

REFERENCES


