SECURITY IN INFORMATION SYSTEMS: SOCIOTECHNICAL ASPECTS

Prof. Edison Luiz Gonçalves Fontes, CISM, CISA – GTECH – São Paulo - SP/BR –
edison@pobox.com
Prof. Antonio José Balloni – CenPRA/MCT – Campinas – SP/BR –
antonio.balloni@cenpra.gov.br

Abstract - This work considers the sociotechnical approach that must be addressed when implanting and having maintenance of the information security of an organization. In general, only the technical aspects are considered by the IT professionals. These technical aspects generates in the organization in the day by day, a security process that seems as a set of distant rules and, because of this, the security process (the rules) will not be internalized by the users. To consider sociotechnical aspects means both making a complete approach for the security subject as well increasing the chances for the existence of a continuous process, following and protecting the information resources during the growing stages and moments of difficulties in the organization.

I. INTRODUCTION.

The security in information systems must contemplate not only the technical aspects. The social aspects related to the organization environment and related to the people also have its importance and must be considered.

Due the fact that, historically, the information security began from the technical area of data processing then, the social aspects of the organization and the people have been left of side. Another important fact that must be considered is that even the technical aspects possess a ampler connotation ***[01].*** Furthermore, while security breaches and damage to information systems still come from organizational insiders, security breaches from outside the organization are increasing because firms pursuing electronic commerce are open to outsiders through the Internet. It is difficult for organizations to determine how open or closed they should be to protect themselves. If a system requires too many passwords, authorizations, or levels of security to access information, the system will go unused. Controls that are effective but that do not prevent authorized individuals from using a system are difficult to design.

This work present a approach for information system security that surpass the technical aspect warning the managers from information security as well as the executives of the organizations that the protection of information resources must consider the sociotechnical perspective.

II. SOCIOTECHNICAL SECURITY INFORMATION SYSTEM: DEFINITIONS.

3.1 - Socials concerns:

These are the aspects strongly related to peoples and to the environment where these peoples live and work.

3.2 - Technical concerns:

They are the aspects strongly related to the technology and to the resources of technology.

3.3 - Sociotechnical perspective:

In a sociotechnical perspective the performance of a information system security is optimized when both the technology and the organization mutually adjust to one another until a satisfactory fit is obtained ***[02]***.

III. PLANNING THE SECURITY OF INFORMATION: SOCIOTECHNICAL DESIGN.

For implementing a information security process it is primordial the elaboration of a planning but, what about the information security?

- Information security: whereas information security used to be an arcane, technical topic, even CEO know about it today due to importance of electronic information in running their business. Actually, all business executive now need to understand Internet-based threats and countermeasures and continually fund security work to protect their businesses. At first, when government and industry became aware of the need to secure their information resources, attention was focused almost exclusively on protecting the hardware and data and the term system security was used. This narrow focus was subsequently broadened to include not only hardware and data, but also software, the computer facilities, and personal as well. Today the scope is even broader, to include all types of data. The term information security is used to describe the protection of booth computer and non computer equipment, facilities, data and information from misused by unauthorized parties. This broader definition includes such equipment as copiers and fax machines, and all types of media, including paper documents ***[03]***. These aspects, forcedly, forward to a Sociotechnical design.

T. Sobh (ed.), Innovations and Advanced Techniques in Computer and Information Sciences and Engineering, 163–166.

- A sociothecnical design is a design to produce

information systems that blend technical efficiency with sensitivity to organizational and human needs i.e., a sociotechnical design plan establishes human objectives for the system that lead to increased job satisfaction. Designers set forth separate sets of technical and social design solutions. The social design plans explore different work group structures, allocation of tasks, and the design of individual jobs. The proposed technical solutions are compared with the proposed social solutions. Social and technical solutions are, therefore, a sociotechnical solutions. The alternative that best meets both social and technical objectives is selected for the final design. The resulting sociotechnical design is expected to produce an information system security that blends technical efficiency with sensitivity to organizational and human needs, leading to high job satisfaction. Systems with compatible technical and organizational elements are expected to raise productivity without sacrificing human and social goals ***[04]***.

3.1 – Guidelines to Information Security.

The goal of Information security is to achieve the following objectives: confidentiality, availability and integrity. Confidentiality: the firm seeks to protect its data and information from disclosure to unauthorized persons. Availability: The purpose of the firm's information infrastructure is to make its data and information available to those who are authorized to use it. Integrity: data with an unreduced or unbroken completeness ***[05].***

Next lets consider the main item necessaries when implementing a planning for a information security process.

The security of the information is rich in operational activities and, as function of its weaknesses, we are guided to, immediately, start with technical actions which are, at first, considered as the "most important". However, there is an potential hazard if we are only limited to these operational activities! As the operational activities are an important elements for the organization then, it is very important having an elaborated Information Security Strategic Planning (ISSP) and, this ISSP must be validated by the high administration of the organization, guiding the ways that the projects and activities must follow.

The basic guidelines for implementing the ISSP to be followed are:

a) being aligned with the organization's politics and legislation.

All actions for security of the information must respect the actual state legislation as well the organizational politics.

b) considering the business initiatives.

The most important action for the businesses of the organization is its accomplishment, i.e, the survival from the enterprise. Therefore, for the accomplishment of a viable business, the security must guarantee that the information use in the several initiatives of that business, is happening in a adjusted way. At the same time, an extreme protection can make a nonviable business.

c) defining the structure of a security area.

Should we use ours humans resources for ours projects or, the human resources from others areas? How the scope of the Information System (IS) becomes in the organizational structure? How these and others definitions regarding the area of security need to be predefined?

d) defining the operation form.

Together with the structure definition it is necessary to mount the operation form and scope area of the information security. In general, the computational environment must be contemplated but, depending on the kind of organizations, several subjects as equipment protection, environment and peoples etc, should also be cared for since these subjects are in a gray area.

Following these basic guidelines, a good strategy must be divided into three components: Architecture, Commitment and Protection actions

- *Architecture.*

The security process of the information must follows a viable (possible to be carried out) architecture ***[06]***. In terms of protection approach, this architecture allows a complete vision of a practical architecture ***[07]***.

- *Commitment.*

The user commitment is the support (pillar) for the organizational information security effectiveness.

- *Protection actions.*

Here fits in all the procedures, technical or not, that will drive the protection of the information. Sometimes we are compelled to consider only this approach: protections actions.

This practical example, figure 1, of strategic planning is not a closed rule therefore, it must be applied based on necessaries adaptations for the reality of your organization.