Chapter 6
Information Security Policy: The Regulatory Basis for the Protection of Information Systems

Edison Fontes
Faculdade de Informática e Administração Paulista (FIAP), Brazil

Antonio José Balloni
Centro de Tecnologia da Informação Renato Archer (CTI), Brazil

ABSTRACT

In this chapter, the reader finds a structured definition to develop, implement, and keep the needed regulatory rules or principles for an Information System Security (ISS). In addition, the reader finds how to ensure the right use of this ISS, as well as in authorization and protection against disaster situations such as an effective system protection when accessing, storing, using, and retrieving the information in normal or contingency situations. This compound is the structure of information security policy that is based on a set of controls as described in NBR ISO/IEC 27002 (ABNT, 2005). The definition of this structure for the information security policy is important because the Norm ABNT (2005) does not indicate nor define—nor explain—how the structure of this policy should be (i.e., which are the fundamental elements and functions, which are the standards of rules for the controls and other practical issues) so that the policy could be effective for the organization. The structure shown in this chapter represents a practical and useful architecture regarding the elements of the information security policy of the organization.

INTRODUCTION

This chapter describes a structure for the information security policy with the objective of facilitating the elaboration of a set of regulations of the organization which comprises this policy. So, this information security policy structure aims to facilitate the development of this set of regulation.

The NBR ISO/IEC 27002 (ABNT, 2005) (Information Technology (Security Techniques) Practice Code for Information Security Management) requires the need of information security policy, but the Norm does not indicate how the regulation or regulations, which make up this policy, should be structured.

It is desirable that the directions of the organization establishes a clear political guidance aligned with the business goals, and demonstrate support and commitment with the information security

DOI: 10.4018/978-1-4666-6320-6.ch006

through the publication and maintenance of an information security policy for the entire organization. (ABNT, 2005)

To prepare an information security policy is a difficult task for the organizations. A tangible example was recorded in organizations that deal with health data, and which do not yet have their policies for information security in spite of their executives understanding of the importance of regulations for information security. Albertin and Pinochet (2010) in their research "Cycle of continuous monitoring for the development of information security policy in hospital organizations", described the survey in five hospitals in the State of San Paolo, Brazil, where in all of them, in a direct or indirect way, the managers declare the importance of information security, but none of them had an appropriate information security policy. Declarations from managers of such hospitals demonstrate the difficulty that these organizations have to generate an information security policy:

The hospital has a serious lack in developing information security policy. (Albertin and Pinochet, 2010).

The managers, in their majority, consider there is a lack of knowledge regarding how to map the needs to develop a formal information security policy. (Albertin and Pinochet, 2010).

The hospital has clear shortcomings in developing information security policy due to lack of guidance from the Secretary (of State) and the board of health. (Albertin and Pinochet, 2010).

According to Picovsky (2012), it is, therefore, necessary the proper and suitable use of information systems, aiming to improve the quality and safety of health care at lower cost. Yet, according to Morales (2007), all of the information that a physician may need should be available in the charts of the patient and, therefore, it is necessary to guarantee security in obtaining this information. This shows clearly the issue and need of a security system -information security policy-.

A survey conducted by Consultancy PriceWaterhouseCoopers (2011), CIO Magazine and CSO Magazine shows policies for information security is an ongoing concern. This study represents a unified data analysis regarding the information provided by more than 12,800 executives, among CEOs, CFOs, CIOs, CSO, and vice presidents, directors of IT and information security officers from medium, large and giant enterprises from 135 countries and all sectors. About 500 of these executives were from Brazil.

In spite of the world crises regarding information security (as described in the survey), the PriceWaterhouseCoopers (2011) document also presents a compliance with the organization internal policies for information security and the resources with information security process as one of the five most important factors. The other factors were identified as: economic conditions, business continuity/disaster recovery, company reputation and regulatory compliance.

The authors believe the investment in information security is dragged/pulled by five items above mentioned: the information security policy requires the organization to implement actions in such a way that the organization is in compliance with the security rules. In this way, the compliance with the policy and other organizational internal rules becomes a driver/(give directions) towards the spending of resources in information security.

In the year 2013, the PricewaterhouseCoopers (2013) carried out a new research. This time there were 575 executives from Brazil and 9,300 executives from others countries. The survey showed 68% of respondents understand the major challenge of an organization is the establishment of a Security Corporative Strategy. This research indicates that executives need structures which guide them how to implement an information security process; i.e. the executives need guidance