Information Security and Data Controllability for Collaborative Systems

Manuel Munier
LIUPPA, EA 3000
Universite de Pau et des Pays de l'Adour, E2S UPPA
Mont-de-Marsan, France
e-mail: manuel.munier@univ-pau.fr

Vincent Lalanne
LIUPPA, EA 3000
Universite de Pau et des Pays de l'Adour, E2S UPPA
Pau, France
e-mail: vincent.lalanne@univ-pau.fr

***Abstract*—The new information and communication technologies have brought an evolution of IT systems from a standalone architecture to architectures where the systems are interconnected, and this in a multi-organizational environment. Through their interactions and their collaboration with external systems, notably via the service paradigm, information systems have become the place where information from different sources converges: data collected by the information system, computed data, data from outsourced services or databases,... Therefore, from a computer security point of view we can no longer focus solely on hardware, software and network issues. From now on, we must take into account the data that is an integral part of an organization's capital: data is today the main concern of companies. In this article we address the information security from the perspective of risk management taking into account the ability of an organization to control its data flows (incoming and outgoing). We propose the introduction of a new security criterion: the "controllability". The consideration of this criterion is essential to avoid the garbage in, garbage out issue (incoming data) and to reduce the risks in the use of the data produced (outgoing data).**

Keywords*—*data quality; information security; controllability; risk assessment; services; collaboration;

I. Introduction

Nowadays, whatever their sector of activity, information has become the center of concern for companies. This concerns not only their informational capital as such, but also all information flows in and out of the company. We are now in a (digital) information society where some companies produce information while others are consumers.

In this context, the information system (IS) is the nerve center of companies. If its constituent elements (personal, hardware, software,...) make it possible to acquire, process, store and communicate information. But the main purpose of an IS is no longer limited to being a "shared storage". Depending on the level of maturity of companies with respect to their information capital, the IS function can go beyond the role of support function (operational level, data warehouse, collaborative platform) and position itself as a business partner (decision-making function, economic intelligence). Companies must consider all factors related to the effective use of information. This is all the more true in the context of collaborative systems. For this, the current forms of IS governance must evolve to explicitly take into account the use of information, especially from the point of view of information security.

And in our opinion, information security can no longer be based solely on computer security mechanisms (hardware, software, networks,...). We have to take into account qualitative and organizational criteria to have a global approach to information control in the company. In this article we propose a new security criterion, the controllability, to evaluate the ability of the company to control its information following a risk management approach related to the information security.

This article is structured as follows. Section II introduces various tools for information security, as well as the limitations of traditional security criteriawith respect to our need for information (value) control. Section III provides an overview of some of the work related to data quality management. In section IV we propose a new criterion, the controllability, to quantify the level of control of an organization in the information it handles. The definition of this criterion is based on a risk management approach by presenting the vulnerabilities, threats and risk scenarios associated with this criterion. Finally, section V concludes this article by mentioning some possible perspectives for this work.

II. Information Security Tools

In this section we will briefly remind the three basic security criteria, namely confidentiality, integrity and availability. Other concepts such as traceability and accountability have subsequently been introduced in risk management methods to formalize other aspects of information security.

A. Key concepts

The information system is an essential asset of the organization, which should be protected. IT security is to ensure that an organization's hardware or software resources are only used within the intended framework [1]. To define the security of information, it is necessary to study its two components:

- **The information**, which can be presented whatever its form of storage, processing or transmission. Here we can talk about a piece of paper, an oral exchange, a binder, a digital structure coupled with a method of transmission by telecommunications...
- **Security**, evaluated by various defined criteria that qualify the security of information.

Security can indeed be qualified by different elements. We are talking here about CIA triad (for Confidentiality,