Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 179 (2007) 47–58
www.elsevier.com/locate/entcs

Security and Trust in IT Business Outsourcing: a Manifesto[6]

Y. Karabulut[1] [a], F. Kerschbaum[2] [a], F. Massacci[3] [b], P. Robinson[4] [a] and A. Yautsiukhin[5] [b]

[a] SAP Research, Karlsruhe, Germany
[b] DIT, University of Trento Trento, Italy

Abstract

Nowadays many companies understand the benefit of outsourcing. Yet, in current outsourcing practices, clients usually focus primarily on business objectives and security is negotiated only for communication links. It is however not determined how data must be protected after transmission. Strong protection of a communication link is of little value if data can be easily stolen or corrupted while on a supplier's server. The problem raises a number of related challenges such as: identification of metrics which are more suitable for security-level negotiation, client and contractor perspective and security guarantees in service composition scenarios. These challenges and some others are discussed in depth in the article.

Keywords: Business Process Outsourcing, Security, Security Metrics, Protection Level Agreement.

1 Introduction

Today many companies prefer to delegate IT work packages to external or third-party organizations rather than fulfilling them themselves [4,11]. In this way a company can concentrate on its core business rather than on peripheral tasks, especially if they differ too much from the company's primary activities. For example, Consolidated Freightways, a transportation company, outsources the upgrade and management of its IT infrastructure to IBM Global Services [11].

[1] Email: yuecel.karabulutATsap.com
[2] Email: florian.kerschbaumATsap.com
[3] Email: Fabio.MassacciATunitn.it
[4] Email: philip.robinsonATsap.com
[5] Contacting author. Email: evtiukhiATdit.unitn.it
[6] This work was partly supported by the projects: EU-IST-IP-SERENITY (N 27587), MIUR-FIRB-ASTRO (N RBNE0195K5), PAT-MOSTRO (2003-S116-00018), IST-FP6-FET-IP-SENSORIA (N 016004)

doi:10.1016/j.entcs.2006.08.030

Definition 1.1 *Outsourcing* is the ongoing administration, management and possibly subcontracting by an external party, of specific client's (IT) processes to enhance their efficiency and effectiveness [25]

Often the outsourced company itself may further outsource its assignments to others. That is, a company may start as a contractor and by acquiring and handing out new assignments may become an orchestrator.

When a company plays an orchestration role it coordinates a business process to accomplish the work. The process can be static or dynamic. In traditional outsourcing contracts we envisage a static orchestration where the process is defined from the outset and partners and services do not change. For novel paradigms, such as virtual organizations, partners and services can be selected on the fly.

Before cooperation proceeds, participants negotiate a *Service Level Agreement* (SLA). The main part of the agreement is devoted to functional requirements and to some non-functional requirements such as performance. Not enough attention, if any, is devoted to security.

Example 1.2 Web Service security only focuses on the security parameters of communication links. It covers requirements for message encryption, signature, authentication, and server access control [2,23]. WS security standards do not mention how data is protected after transmission. Data can therefore be stored in a server without a properly configured antivirus or in a database without role base access control.

In this paper we identify the security and trust issues that underpin an outsourcing relationship and the notion of *Protection Level Agreement* (PLA) that is appropriate in this setting.

The paper is organized as follows. Section 2 is a short state of the art in security metrics. We introduce a notion of PLA in Section 3. Sections 4 and 5 are devoted to client's and contractor's view of PLA respectively. Section 6 describes how client's PLA can be achieved in service composition scenario. The issue that trust is not transitive is discussed in Section 7. Section 8 is dedicated to related works.

2 Security Metrics. A Primer

Unclear performance and benchmarking metrics are a cause of 56% of outsourcing relationship failure [31]. Therefore, the first step in the problem solution is security metrics identification, a task that so far remained elusive.

Loosely speaking all metrics can be classified into one or more of the following categories:

Organizational - evaluate the security management process.

Operational - assess the system and operating principles in place

Technical - evaluates the quality of software and hardware.

The most well known technical method are the Common Criteria [15]. A product