Engineering Security Agreements Against External Insider Threat

Virginia N. L. Franqueira, Department of Computing, University of Central Lancashire, Preston, UK
André van Cleeff, Department of Computer Science, University of Twente, Enschede, The Netherlands
Pascal van Eck, Department of Computer Science, University of Twente, Enschede, The Netherlands
Roel J. Wieringa, Department of Computer Science, University of Twente, Enschede, The Netherlands

ABSTRACT

Companies are increasingly engaging in complex inter-organisational networks of business and trading partners, service and managed security providers to run their operations. Therefore, it is now common to outsource critical business processes and to completely move IT resources to the custody of third parties. Such extended enterprises create individuals who are neither completely insiders nor outsiders of a company, requiring new solutions to mitigate the security threat they cause. This paper improves the method introduced in Franqueira et al. (2012) for the analysis of such threat to support negotiation of security agreements in B2B contracts. The method, illustrated via a manufacturer-retailer example, has three main ingredients: modelling to scope the analysis and to identify external insider roles, access matrix to obtain need-to-know requirements, and reverse-engineering of security best practices to analyse both pose-threat and enforce-security perspectives of external insider roles. The paper also proposes future research directions to overcome challenges identified.

Keywords: Business Network, Conceptual Modelling, Extended Enterprise, Inter-Organisational Network, Security Analysis, Security Management, Service Level Agreement

INTRODUCTION

In the past, companies were loosely linked only to a few other companies and their IT resources, i.e. IT infrastructure, data and business processes, remained in-house under their custody and control. Today, companies no longer operate in isolation but are rather tightly connected to other companies in a network-like structure, called business networks, inter-organisational networks or extended enterprises (Wiendahl & Lutz, 2002; Jagdev & Thoben, 2001; Baraldi et al., 2012; Hakansson & Ford, 2002), with different levels of integration and cooperation.

DOI: 10.4018/irmj.2013100104
Extended enterprises are ever more attractive because they provide competitive advantage by allowing cost savings, time and quality-related benefits, and by increasing business agility and flexibility; each participant in an extended enterprise specializes on its core competencies and takes advantage of other organisations’ expertise to deliver its business mission (Jagdev & Thoben, 2001; Starr et al., 2003). The growth in the adoption of Cloud Computing and the diversity of service bundles on offer exacerbate the fact that organisational boundaries in an extended enterprise context are overwhelmingly fuzzy (Jericho-Forum, n.d.; Thoben & Jagdev, 2001; Jagdev & Thoben, 2001). The size of an extended enterprise can be significant, typically reaching hundreds; research from the Information Security Forum indicates that, on average, companies work with 750 service providers (Davis, 2010). This adds-up to other factors, such as the complexity of dependencies among participants of the network, geographic dispersion, and distributed sources of risk (Thoben & Jagdev, 2001; Davis, 2010), and to the fact that each company part of an extended enterprise is most likely to be itself an extended enterprise, creating a chain of non-transparent B2B relationships.

Extended enterprises create a security management problem in part because it is difficult to have a holistic overview of security across systems, technologies and resources in the entire network. One specific sub-problem of security management in extended enterprises is what we call the external insider threat. Such threat is posed by a class of individuals employed by participants of a company’s extended enterprise network – or their network – who need access to a certain extent to the assets (e.g., data, IT infrastructure, processes) the company owns and is accountable for, regardless of where and by whom it is handled. External insiders are a class of individuals which do neither completely fall under the class of insiders nor of outsiders of one company, and therefore, mitigations to insiders and outsiders do not completely solve the external insider threat problem. External insiders of a company assume a large number of roles across numerous other companies part of its extended enterprise in a variety of B2B arrangements. Those arrangements involve different levels of integration, cooperation and resources sharing (Kumar & van Dissel, 1996; Jagdev & Thoben, 2009). They can span from more traditional arrangements such as trading partners in a value chain, service providers, business partners, to less traditional arrangements such as outsourced operations or facilities providers, security managed providers, Federated Cloud service providers (Bernsmed et al., 2011), or even innovation-driven cooperatives (Thorgren et al., 2009) and consortia for collective management of security (Gupta & Zhdanov, 2007).

A recognized way to mitigate risks and enforce trust in B2B relationships is to formalize agreements via contract. For example, umbrella agreements (also called framework agreements) are an often chosen type of contract as the complexity of such relationships increase (Mouzas & Ford, 2002). They provide a framework of norms but “remain sufficiently flexible to respond to unforeseen contingencies and embrace new or emerging business opportunities” (Mouzas & Ford, 2012, p. 154). Quality of Service (QoS) thresholds, and corresponding penalties, may be established via Service Level Agreements (SLAs) to specify measurable standards of service, which complement umbrella agreements. However, QoS parameters are typically related to service performance, availability and reliability, while non-quantifiable security requirements for service assurance remain an open issue in SLAs (Jaatun et al., 2012; Morali & Wieringa, 2010) due to challenges already discussed in the late 90’s (Henning, 2000) and only intensified by emerging B2B relationships. Security SLAs, often called Protection Level Agreements (Krabulut et al., 2007), must cover the protection of data during its whole lifecycle and must be negotiated between parties. This is our solution direction to counter the external insider threat.

We take the point of view of one company in an extended enterprise, which we call the focal company or focal organisation, through the
Related Content

Social Engineering: The Neglected Human Factor for Information Security Management
[www.igi-global.com/article/social-engineering-neglected-human-factor/55064?camid=4v1a](www.igi-global.com/article/social-engineering-neglected-human-factor/55064?camid=4v1a)

Mobile Number Portability in an Asymmetric Telecommunications Market: Korea Case
[www.igi-global.com/chapter/mobile-number-portability-asymmetric-telecommunications/20626?camid=4v1a](www.igi-global.com/chapter/mobile-number-portability-asymmetric-telecommunications/20626?camid=4v1a)

Database Technologies on the Web
[www.igi-global.com/chapter/database-technologies-web/14329?camid=4v1a](www.igi-global.com/chapter/database-technologies-web/14329?camid=4v1a)
Technology Exploration Process: From Technology to New Services
www.igi-global.com/chapter/technology-exploration-process/21644?camid=4v1a