Chapter 72
Trust in an Enterprise World: A Survey

Fotios I. Gogoulos
National Technical University of Athens, Greece

Georgios V. Lioudakis
National Technical University of Athens, Greece

Anna Antonakopoulou
National Technical University of Athens, Greece

Dimitra I. Kaklamani
National Technical University of Athens, Greece

Iakovos S. Venieris
National Technical University of Athens, Greece

ABSTRACT

Web 2.0 technologies have fundamentally reshaped everyday users' perceptions regarding online services by strengthening the importance of individual participation. This profound change is expanding to substantially affect modern enterprise operations and especially corporate information management practices. Well-established business models are upgraded to capture value from the establishment of dynamic coalitions and virtual organizations among remote stakeholders. However, these collaboration formulations dictate the concentration, use, and circulation of corporate information and sensitive personal data, and thus ignite severe security and privacy concerns. Enterprises against this background are more than willing to invest in terms cost and time in order to enforce the necessary countermeasures and thus build and maintain the trustworthiness of involved operations. This chapter studies how legislation and inherent characteristics of this new collaboration paradigm affect the qualities of trust and highlights prominent features of security and privacy protection measures that can deal with emerging trust issues.

INTRODUCTION

Recent advances in information technologies are fundamentally reshaping the modus operandi of online markets around the globe. Enterprises on intra and inter organizational level are moving from monolithic client-server architectures towards dynamic clouds of resources. Collaborative Web 2.0 technologies have become the leading edge of this rapid transformation and have set the foundation for the emergence

DOI: 10.4018/978-1-5225-8897-9.ch072

of a new business operation and collaboration paradigm labeled as Enterprise 2.0. The term Enterprise 2.0 coined by (McAfee, 2006a) as the adoption of Web 2.0 services to improve knowledge workers' productivity and augment the effectiveness and competence of organizations does not necessarily embrace explicit technological tools; it rather introduces a groundbreaking model for an enterprise's knowledge structure, information management and resources sharing.

Determinants in the process of Enterprise 2.0 adoption constitute the empowerment of users, the bottom-up formulation of new processing patterns, the emergence of free-flowing collaborative engagements, and the effective guidance of possible participants (De Hertogh, Viaene & Dedene, 2011). That is, Web 2.0 initiatives call for a profound shift of dynamics from a top-down to a bottom-up business logic; business value is built collectively by knowledge workers and is not simply imposed from a small number of key stakeholders. In this context, emerging electronic transactions have become highly dynamic in their nature, while involved work and data flows are suffused over totally decentralized collaboration parties employing distinct roles in the service provision chain.

However, inherent characteristics of the 2.0 epoch described above can ignite severe trust issues among participating entities. Whereas enterprises traditionally enforce strict centralized controls regarding information access and dissemination in the context of emerging transactions, openness and collective participation attributes of Web 2.0 tend to pose significant information security and individuals' privacy risks and thus call for immediate action. In a time where European citizens declare their concerns regarding their personal data and private life protection (Gallup Organization, 2008; European Opinion Research Group, 2011), it becomes evident that it is the level of user's trust and confidence regarding these emerging technologies that can either boost their applicability and effectiveness or comprise a heavy obstacle in the way of their diffusion.

On an international level, companies involved in e-business transactions have reached this realization; while exposing their resources through collaboration initiatives the respective potential information security and confidentiality attack surface is widened. Ultimately, the key to the successful and beneficial adoption of Enterprise 2.0 is acquiring the appropriate balance between vast user empowerment and strict privilege control. Against this background, information security and privacy as means to instill trust into potential collaborators has become a salient issue for enterprises and their key personnel in the 2.0 era (Milojicic, 2008). Evidently, along with trustworthiness privacy and security measures bring commercial value to organizations, a value greatly enhanced by the fact that privacy is increasingly becoming a legislated area. Awareness of the public regarding personal data protection, strengthened by legislation on an international level, affects collaborators' online behavior when involved in commercial activities (Acquisti, 2010) and thus motivates enterprises to adopt appropriate business models. In this climate, a number of keynote information security specifications and standards issued by leading institutions further intensify the organizations' perception of trust and sensitivity about risks stemming from privacy infringement and security breaches.

Ultimate objective of this chapter is to provide a concrete theoretical and technological roadmap for trust in the 2.0 era; from privacy and security related legislation and Web 2.0 operation patterns to explicit trust requirements and from the latter to compliance through respective technical trust management approaches and solutions. Major information security standards, privacy related legislation, along with the particularization of trust in Enterprise 2.0 environments and the specification of trust requirements comprise the content of the next section. The chapter then delves into the literature and