The Enterprise 2.0 Concept: Challenges on Data and Information Security

Ana Silva[1], Fernando Moreira[2], and João Varajão[3,4]

[1] EGP – University of Porto Business School, Portugal
[2] University Portucalense, Portugal
[3] University of Trás-os-Montes e Alto Douro, Portugal
[4] Centro ALGORITMI, Portugal
anamachadosilva@gmail.com, fmoreira@uportu.pt, jvarajao@utad.pt

Abstract. The Web 2.0 wave has "hit" businesses all over the world, with companies taking advantage of the 2.0 concept and new applications stimulating collaboration between employees, and also with external partners (suppliers, contractors, universities, R&D organizations and others). However, the use of Web 2.0 applications inside organizations has created additional security challenges, especially regarding data and information security. Companies need to be aware of these risks when deploying the 2.0 concept and take a proactive approach on security. In this paper are identified and discussed some of the challenges and risks of the use of Web 2.0 tools, namely when it comes to securing companies' intellectual property.

Keywords: Enterprise 2.0, Web 2.0, security, data, information.

1 Introduction

What started as a Web phenomenon, much led by the proliferation of social networks and the growing use of tools such as *blogs*, *wikis* and *mashups*, is now gaining wide acceptance at an enterprise level. Several companies are beginning to understand the benefits that the Web 2.0 concept and tools can bring in terms of internal collaboration, staff engagement and knowledge sharing.

Tim O'Reilly, as cited by Ross Dawson (2009), views the Web 2.0 as "the business revolution in the computer industry caused by the move to the Internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: build applications that harness network effects to get better the more people use them."

Users started experiencing the advantages of the Web 2.0 tools in their personal life recently, connecting with friends on social networks, sharing their views through *blogs* or collaborating through *wikis*. Concepts such as *commenting*, *microblogging*, *tagging* and *rating*, became part of their "regular" vocabulary.

But soon users began to make use of these tools to connect with co-workers, or with other people sharing the same interests, on more "professional" social networks such as *LinkedIn*. They started sharing work documents through *web applications*

M.D. Lytras et al. (Eds.): WSKS 2010, Part I, CCIS 111, pp. 363–368, 2010.

such as *Google Docs* or using their personal email accounts for professional reasons because they find these web-based email services much more appealing and flexible. And it did not take long before people started demanding, inside their companies, the same user experience, tools and networking.

With the blurring of the frontier between personal and professional use of web-based tools companies are currently facing additional security challenges, namely in what concerns the protection of intellectual property. In this paper we will reflect on some of these challenges and risks and provide some guidelines for managing them.

Following, in section 2, are discussed the implications of the Web 2.0 phenomenon for enterprises. In section 3, are identified some of the main challenges of Enterprise 2.0 on data and information security. Section 4 is about security recommendations. Finally, in section 5, some final remarks are made.

2 Implications of the Web 2.0 Phenomenon for Enterprises

Citing an example from the United States, Jim Till (2008) pointed that "researchers estimate that more than half of US employees abandon enterprise tools when they need to work with applications outside of their organization to complete a project or task." And a recent press release from IDC (2010), highlighting some key findings of a research on the intersection of the topics of Web 2.0, Enterprise 2.0 and collaboration, stated that last year "57% of U.S. workers use social media for business purposes at least once per week".

As companies began deploying the Web 2.0 concept and tools inside their organizations, the notion of Enterprise 2.0 emerged. This is a term largely attributed to Andrew McAfee (2006) that described it as "the use of emergent social software platforms within companies, or between companies and their partners or customers."

Today, if someone was asked to give a definition of Enterprise 2.0, it would probably be something like "the deployment of Web 2.0-style tools and practices with the purpose of fostering collaboration and collective intelligence inside organizations". The concept has to go beyond technology in order to truly reflect a new way of working and collaborating, both inside (between co-workers) and outside (with partners) the company.

At the moment the question for several companies, especially the larger ones with a wide geographic present, does not seem to be whether or not to deploy the Enterprise 2.0 concept, but rather when and how.

As Ross Dawson (2009) referred "key issues in adapting Web 2.0 tools to the enterprise include scale, IT security, identity, information loss, and auditability." And in the latest Enterprise 2.0 conference, Whitney Michael (2009) published a small article where it highlighted that security concerns were appointed, by 31,5% of respondents to a survey conducted in May 2009, as the greatest challenge in E2.0 adoption.

Dawson (2009) summarized the main risks and concerns usually associated with the implementation of the Enterprise 2.0 concept, categorizing it in: security; loss of control; reputation; and reliability. But the author also points to the risks of taking no action, such as the unauthorized use of external tools to perform work tasks, leading to IT security risks and lack of integration with existing systems, or the scattering of information with users placing information outside a coherent firm structure.