Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
International Journal of Information Management 25 (2005) 85–98
International Journal of
Information
Management
www.elsevier.com/locate/ijinfomgt

Case study

# Securing knowledge in organizations: lessons from the defense and intelligence sectors

Kevin C. Desouza[a,*], Ganesh K. Vanapalli[b]

[a]*Department of Information and Decision Sciences, University of Illinois at Chicago, 601 South Morgan Street, M/C 294, Chicago, IL 60607, USA*
[b]*Indian Navy, Naval Headquarters, Sena Bhavan, New Delhi, India*

**Abstract**

The interest in the field of knowledge management continues to grow at an astounding rate. An organization must leverage its core competencies, which are mostly knowledge-based resources, in order to survive and thrive in the current marketplace. While there are many studies addressing how one should leverage knowledge assets, the work on how we can secure our existing knowledge assets and processes is scant. While private sector organizations have long taken knowledge security for granted, this is not the case in the intelligence and defense sectors of the government, especially those involved with issues of national security. In this case study analysis, we will draw on key insights from investigating knowledge security protocols in five such organizations. This case study takes the first steps towards investigating the security dimension of knowledge management.


*Keywords:* Knowledge management; Security; National security

## 1. Introduction

Knowledge management, as a discipline, has moved from a fad to a necessity to compete in today's marketplace. As postulated by the knowledge-based view of the firm, knowledge the organization possesses is the most salient source of sustainable competitive advantages

*Corresponding author. Tel.: +1 312 829 8447; fax: +1 312 413 0385.
*E-mail address:* kdesou1@uic.edu (K.C. Desouza).

0268-4012/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2004.10.007

(Kogut & Zander, 1992). The current literature on knowledge management has examined the questions of how, why, when, and where to leverage knowledge assets (see, for example, Davenport & Prusak, 1998; Nonaka & Takeuchi, 1995). While this line of thinking is apt for helping us gain an understanding of how to derive value out of knowledge assets by exploiting them to their full potential, it ignores a rather salient question—how can we secure our existing knowledge assets?

Knowledge possessed by an organization must be protected and made scarce to the external world, in order for an organization to remain competitive. Unless we have apt security measures in place we risk losing them to acts of theft, misuse, espionage, and disasters. Securing knowledge assets is even more important given the current economic, social, and political conditions, such as the surge in terrorist activities. While private sector organizations have long taken knowledge security for granted, this is not the case in the intelligence and defense sectors of the government, especially those involved with issues of national security. We draw on our examinations of knowledge management practices conducted in organizations belonging to the defense and intelligence sectors (DIS) of the government. It is our belief that an exposure to these lessons will help private organizations better their knowledge management security practices.

We have gleaned salient lessons learnt from conducting multiple case studies in several DIS organizations. We begin by remarks on our research methodology. Next, we detail our findings and their implications. Concluding the case study is a look at managerial and scholarly avenues for further investigations into security aspects of knowledge management.

## 2. Case methodology

We conducted case studies at five DIS organizations; the primary goal of these organizations is to protect the national security of their respective countries. Three of the organizations are based in the United States, one each in Asia, and Europe. We conducted interviews with over 30 senior personnel at the various agencies, reviewed documents and manuals, engaged in on-site observations, and even elicited data using open-ended surveys (Klein & Myers, 1999; Eisenhardt, 1989). The data collected helped us gain an understanding for both the espoused security practices and those that were in use. The rich array of data collection methods provided us an optimal way to triangulate our findings and check for conformity and validity. Once analysis of data was completed, we presented our findings to members of the DIS organizations to receive feedback and seek their input on items that were still high in equivocality. We composed case studies (sometime two or more from an organization) to document peculiar and unique practices in managing knowledge. In addition to conducting primary data collection, we also reviewed the extant literature on security management in DIS organizations. We gathered unclassified material on knowledge management practices underway at the United States Army, Untied States Navy, Central Intelligence Agency, Department of Defense, Department of Energy, Indian Navy, and the US Federal Bureau of Investigations (FBI). For example, we studied the cases on security breaches of Aldrich Ames, Robert Hanssen, Harold James Nicholson, John M. Deutch, and others, to gain insights into security practices at the agencies. We commenced data collection and analysis when it was found that additional data being collected was not adding to our understanding of the core concept (Eisenhardt, 1989).