Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Protecting organizational competitive advantage: A knowledge leakage perspective

Atif Ahmad [a,*], Rachelle Bosua [a], Rens Scheepers [b]

[a] Department of Computing and Information Systems, University of Melbourne, Parkville, VIC 3010, Australia
[b] School of Information Systems, Deakin University, Australia

ARTICLE INFO

Article history:
Received 23 August 2013
Received in revised form
27 November 2013
Accepted 9 January 2014

Keywords:
Knowledge leakage
Information security
Security risk
Sensitive information
Resource-based view

ABSTRACT

The strategic management literature emphasizes the importance of protecting organizational knowledge and information, especially in terms of maintaining competitive advantage. We synthesized several mechanisms from the literature that organizations could deploy to protect their knowledge and information. An Australian field study investigated how and to what extent these mechanisms were deployed in 11 knowledge-intensive organizations. The study revealed surprising findings: firstly, there was no evidence of a systematic and comprehensive management approach to the identification and protection of knowledge assets. Approaches were often haphazard, driven in a bottom-up fashion with much of the responsibility delegated to individual employees and knowledge owners. Secondly, concerns about confidentiality of organizations' operational data (e.g., client details), often crowded out managerial attention to protecting organizations' own knowledge and information assets. Based on these observations, we outline several implications for future research, including the need for more comprehensive frameworks to address knowledge leakage from a strategic perspective.

1. Introduction

In recent years, there has been considerable media coverage of an increasing number of incidents in which sensitive information has been disclosed as a result of leakage. Leakage is becoming a key concern in organizations and also an important area of research. For example, a recent special issue of Information Systems Frontiers was dedicated to the security management of internal data leakage. This issue highlighted several important aspects, including "insiders" who leak data (Farahmand and Spafford, 2013). The leakage of sensitive information through unidentified channels and conduits is a particularly challenging management problem. This problem is exacerbated by the widespread adoption and appropriation of boundary-spanning information technologies such as mobile devices, cloud computing, social media and networking technologies.

Leakage can have a variety of impacts on organizations including reputational damage, loss of revenue, costs arising from breaches of confidentiality agreements and loss of productivity. With considerable restitutional effort, organizations could recover from such incidents. However, where the leakage concerns *knowledge* related to an organization's valuable, rare, inimitable and non-substitutable (VRIN) resources that sustain competitive advantage, recovery can be

[*] *Corresponding author*. Tel.: +61 383441396.
E-mail addresses: atif@unimelb.edu.au (A. Ahmad), rachelle.bosua@unimelb.edu.au (R. Bosua), rens.scheepers@deakin.edu.au (R. Scheepers).

0167-4048/$ – see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2014.01.001

significantly more challenging (VRIN resources are discussed in Barney (1991, 1996), and Mahoney and Pandian (1992)). Knowledge is more than just information and data; it can be described as the 'fluid mix of framed experiences, values, contextual information and expert insight' (Davenport and Prusak, 1998). Knowledge is indispensable for innovation and manifests itself in the form of intangible and tangible knowledge assets. Intangible knowledge assets are embodied in humans while tangible knowledge assets become embedded over time in organizational procedures, routines, processes and documents. Given the highly competitive business environment and continuing pressure within which organizations compete, knowledge assets are vital for organizations to sustain their competitive advantage (Grant, 1996, 1997).

Knowledge leakage occurs when sensitive organizational knowledge such as strategies, policies, product-knowledge, and sensitive client information ends up in the hands of unauthorized parties. Leakage has been defined as '*… the deliberate or accidental loss of knowledge to unauthorized personnel within or outside of an organizational boundary"* (Annansingh, 2005). The definition points out that leakage may occur deliberately or in an uncontrolled unobtrusive way, for example due to human error, inferred facts from knowledge made available through various sources, or poor information management strategies and practices. Additionally, practices that include the offshoring and outsourcing of operations by organizations may lead to the unintentional divulging of sensitive organizational knowledge to unauthorized parties.

In the realm of information systems security, leakage of information and data in computers and networks is addressed through the preservation of 'confidentiality'. Formal and informal measures exist to prevent unauthorized access to information and data (such as security policy, risk management, education, training and awareness) (Dhillon, 2006). In addition, there is a range of technical measures to control access to information (consider authentication mechanisms that use passwords, encryption, logging mechanisms, firewalls and intrusion detection systems).

The literature on mitigation strategies focused on the leakage of sensitive *knowledge* is scant (DeSouza, 2006). A few literature sources mention the importance of knowledge protection in organizations (Bloodgood and Salisbury, 2001; Gold et al., 2001; O'Donoghue and Croasdell, 2009; Thompson and Kaarst-Brown, 2005), but fail to provide pertinent guidance on 1) different types of mechanisms required to protect sensitive knowledge, and 2) strategic and operational guidelines on how sensitive organizational knowledge can be protected.

In this paper we report on a particular set of findings insofar as knowledge leakage mitigation and the challenges faced by organizations in this regard. As the focus is on organizations and competitive advantage in particular, we adopt a knowledge-based view of the organization. Given the significant sharing and transfer of knowledge at different levels in knowledge-intensive organizations, we suggest it may be difficult to reconcile the confidentiality of knowledge with its availability. As such it is important to investigate how organizations actually deal with this dilemma. Therefore, this paper poses the following research question: How can Organizations protect their Valuable, Rare, Inimitable and Non-substitutable knowledge assets? From this, two related sub-questions follow:

- *What key mechanisms exist that can be deployed to protect organizational knowledge assets?* and
- *What challenges do managers face in deploying the various knowledge protection mechanisms to prevent the leaking of sensitive knowledge?*

The paper begins with a literature review aimed at identifying broad perspectives on knowledge protection and associated mechanisms in organizations. Using four key perspectives identified from the literature, a qualitative case study approach was taken whereby managers responsible for knowledge strategy from eleven knowledge-intensive organizations were interviewed on organizational approaches towards reconciling the need for knowledge confidentiality with availability. The findings suggest that organizational knowledge protection is a complex issue that is often overlooked at the management level and left as the responsibility of knowledge 'owners'. Additionally, managerial actions, appropriate strategies and accompanying mechanisms are required to distinguish between protection mechanisms of competitive knowledge as opposed to operational knowledge. Based on these observations, several implications for future research are outlined, including the need for more comprehensive frameworks to address the problem of knowledge leakage strategically.

2. Organizational perspectives on securing knowledge, data and information

2.1. *Strategic management view*

The Resource-Based View of the firm views knowledge as an intangible organizational competitive resource that should be developed and protected in the same manner as other competitive firm resources (Teece, 2009). The synergy between knowledge and firm resources often accounts for its competitive advantage generation potential, in the sense that such synergies tend to be unique and consequently not easily imitated by competitors. Indeed, it has been argued that even though firms may possess similar resources, the ability to generate premium rents emanates from leading firms' ability to better harness their intangible knowledge assets in conjunction with other firm resources, for example, see the Creative Arts case in Barney and Hesterly (2006).

When a firm's competitive advantage derives from a knowledge-intensive resource, clearly this advantage could be eroded when competitors obtain such knowledge. This in turn contextualizes the problem of knowledge leakage for organizations strategically. Leakage, with potentially devastating consequences in terms of competitive advantage, could occur on a number of fronts. First, inadvertent or intentional leakage of knowledge by disgruntled employees (which could occur easily in an increasingly networked society) presents one potential risk. Furthermore, alliances between organizations necessitate some sharing of information between business