Chapter 3 Government as a Partner in Knowledge Management: Lessons from the US Freedom of Information Act

G. Scott Erickson *Ithaca College, USA*

ABSTRACT

This chapter assesses the reliability and predictability of government departments as partners in corporate knowledge management systems. The specific topic is knowledge availability under the US Freedom of Information Act, but the general implications apply to governments at all levels around the world that hold business information, data, or knowledge assets. By comparing processes related to US freedom of information requests across departments and across time, separated by a dramatic change in presidential administrations and attitudes toward governmental openness, this study examines the relative reliability of agency processes. In particular, reports on the handling of confidential business information provide us with specific insights on this topic as do reports on records with personal privacy concerns. In the end, there appears to be little predictability in the process, even with clear instruction from the highest levels. The topic needs more in-depth study, but businesses, at least in the US, should share data, information, and knowledge with the government deliberatively.

INTRODUCTION

Can government be a reliable partner for businesses creating and executing a Knowledge Management (KM) strategy? If government entities are to be a valued and trusted part of a KM network, what kinds of policies and practices need to be in place in terms of handling data, information,

DOI: 10.4018/978-1-4666-4434-2.ch003

and knowledge? Can government partners help organizations to build knowledge assets while also keeping them protected?

One of the key strategic questions for a knowledge management system is the degree to which knowledge should be shared, both internally and throughout a wider external network of partners. The entire field of KM is based on the insight that knowledge has more value if it can be identified and then better managed by leveraging it through wider sharing and distribution. This potential should be balanced, however, by considering the security implications of unfettered access. Wider distribution means more knowledge in more hands, in digital form. When these additional hands are external to the core organization, the issues are even more complex. Firms are well-advised to assess the advantages of greater distribution with the potential disadvantages of proprietary knowledge asset loss (Erickson & Rothberg 2012; Rothberg & Erickson 2005).

Knowledge management, and the companion field of Intellectual Capital (IC), are based on the concept of valuable knowledge assets that can be identified (Bontis 1999) and grown (Zack 1999) by means of a variety of methods (Nonaka & Takeuchi 1995). The nature of the knowledge, in part, determines the best approach, including whether the knowledge is tacit or explicit (Nonaka & Takeuchi 1995; Choi & Lee 2003; Schulz & Jobe 2001), whether the knowledge is specific to a circumstance and/or whether the knowledge might be sticky to the originating firm (Kogut & Zander 1992; von Hippel 1994), as well as whether an organization has the absorptive capacity to learn (Cohen & Levinthal 1990). In addition, trust, culture, and other aspects of the firm add up to social capital, which can also have an impact on the success of a KM system (Nahapiet & Ghoshal 1998).

All of this adds up to circumstances in which knowledge must be shared with partners in order for it to effectively grow. This is true inside the firm (Gupta & Govindarajan 2000) but can also be extended to wider replication of technology (Zander & Kogut 1995) including outside the firm (Teece 1988). Indeed, modern business is emphatically about one network of partners competing against another network of partners. Knowledge management systems today increasingly go beyond the borders of the firm to include key (and sometimes not so key) network partners. The issues of complementary culture and trust still apply but now to external organizations. And when one of those organizations is the government, it's fair to ask about whether it can be trusted to value and protect the knowledge assets in the same way the firm does.

This question has become ever more complicated, with new developments in recent years. Just as knowledge management and the related field of Intellectual Capital (IC) widened the definition of what might be valuable proprietary knowledge assets beyond formalized intellectual property, so the inception of big data, business intelligence, and other analytical processes have clarified the potential of pre-knowledge assets like data and information. Knowledge assets today include not just intellectual capital, as we know it, but precursors from information systems. Businesses have an ever-widening variety of intangible assets cycling through operational and transactional systems as well as in KM installations (Andreou, Green, & Stankosky, 2007). All can be of great value as knowledge or pre-knowledge assets but can also sharply increase an organization's vulnerability to competitor infiltration or other sources of knowledge loss.

Some of these new intangible assets include customer databases. Given promises made to consumers in the process of gathering such data, as well as some applicable laws, organizations need to give some attention to security. Consumer data distributed throughout their networks should be kept secret if the firm has promised to do so. Further, if a business partner in a wider network is responsible for releasing ostensibly private data (or proprietary knowledge assets), that will reflect negatively on future prospects for remaining a partner.

And into this mix comes government. These issues are even more complex when applied to the public sector. Governments manage a great deal of knowledge, information, and data. Governments not only leverage knowledge by sharing throughout a wider network that can include businesses and other government entities, but routinely (and by legal mandate) also share knowledge through 12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/government-as-a-partner-in-knowledgemanagement/80109

Related Content

The Role of Resilient Information Infrastructures: The Case of Radio Fukushima During and After the 2011 Eastern Japan Catastrophe

Hans J. Scholland Akemi Takeoka Chatfield (2014). *International Journal of Public Administration in the Digital Age (pp. 1-24).*

www.irma-international.org/article/the-role-of-resilient-information-infrastructures/112001

Navigating the Dragon: China's Ascent as a Global Power Through Public Diplomacy

Mohamad Zreik (2023). *Global Perspectives on the Emerging Trends in Public Diplomacy (pp. 50-74).* www.irma-international.org/chapter/navigating-the-dragon/327771

Advancing Global Business Ethics in China: Reducing Poverty Through Human and Social Welfare

Ruth Wolfand Monica Thiel (2018). *Examining the Private Sector's Role in Wealth Creation and Poverty Reduction (pp. 67-84).*

www.irma-international.org/chapter/advancing-global-business-ethics-in-china/193142

An Innovative Government Architecture with Semantic Technology

Wout Hofman (2016). International Journal of Public Administration in the Digital Age (pp. 47-65). www.irma-international.org/article/an-innovative-government-architecture-with-semantic-technology/146807

"Problems and Suggestions": Non-Governmental Organisations of Sexual Orientation Minorities in the Context of Turkey and United Kingdom

Erhan Aydin (2017). Handbook of Research on Managerial Solutions in Non-Profit Organizations (pp. 232-252).

www.irma-international.org/chapter/problems-and-suggestions/163757