The confidentiality – integrity – accessibility triad into the knowledge security: a reassessment from the point of view of the knowledge contribution to innovation

Daniela Popescul

Alexandru Ioan Cuza University Iasi

29. June 2011

Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage), June 29-30, 2011, Kuala Lumpur, Malaysia, Editor Khalid S. Soliman, ISBN: 978-0-9821489-5-2, pp. 1338-1345

The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation

Daniela Popescul, "Alexandru Ioan Cuza" University, Iaşi, Romania, rdaniela@uaic.ro

Abstract

The necessity of (re)considering the three main faces of security mentioned in the title of the paper derives from the accumulation of the importance of the knowledge circulating in organizations, with the existence of numerous dangers and threats that target this knowledge, focusing on people as depositaries and users of knowledge. After a general presentation of the knowledge workers characteristics that can be analyzed as potential risks from the point of view of the confidentiality, integrity and accessibility of knowledge, the paper suggests some solutions that spin around the idea, that is, knowledge security is a human problem and not a technical one, and therefore it should be treated as such. The paper is mainly addressed to the managers interested in the use of knowledge in the activity of the organizations they lead, warning them about the sensitive points of the knowledge-related activities, with the dangers associated with them and suggesting them that the traditional informational security mechanisms are not sufficient, that they have to be reanalyzed and improved in knowledge security.

Keywords: knowledge management, knowledge security, knowledge workers, organizational decisions

Introduction

As a resource, we all know that knowledge is infinite, inconsumable (it can be used by several persons simultaneously), and accessible for anybody (the monopoly on knowledge held by specialists is visibly reduced). Nowadays, it means power more than ever, as it is "the key to the economic development in the 21st century" (Alvin Toffler). According to another great visionary, Peter Drucker, knowledge not only replaced the traditional production factors – earth, work or capital – but also exceeded them, becoming the essential component of the economic and social development system nowadays, the Resource (notice the capital "R") itself. As mentioned by Fotache (2002), for an organization, knowledge as a strategic resource is related to its various components: culture and identity, procedures, policies, systems, the organization's documents, and each and every single employee. Knowledge, which gives value to the organization, guaranteeing its market identity, has a complex character and is usually produced as a result of a tremendous effort. At the same time, there is a frequently alleged connection between knowledge and innovation within organizations. Innovation is the engine of growth, it has been argued in a study by Peri (2002), and externalities from existing knowledge are the"renewable" fuel that keeps this engine running. Delgado-Verde, Martin-de Castro and Navas-Lopez (2011) affirm that organizational knowledge assets are key organizational factors responsible for firm innovation, and the innovation capability of a certain firm depends very closely on the organizational knowledge that it possesses. Innovation as output is, undoubtedly, the main concern of all the professionals that deal with knowledge management.

Opposite to this usual superlative presentation, which emphasizes the major role of knowledge in contemporary organization, we can notice the relatively rare preoccupations in order to guarantee the security of knowledge, both at an academic and at a practical level. The lack of specialized literature and of practical advice in knowledge security is the more visible as in the data and information ("raw material" that leads to knowledge) security segment there is an impressive quantity of published articles and volumes, as well as millions of Internet pages that offer the most diverse studies, analyses and security solutions. The concept of "secure knowledge management" is still in the embryonic stage as many organizations wrestle with information overload. While data and information management has been the focus of significant research in the information systems field, the interest in knowledge is relatively new. Randeree (2006) mentions that information systems researchers are currently looking at knowledge creation, knowledge acquisition and knowledge sharing, but have yet to focus their attention on protecting and securing knowledge. This is a paradox, because, as said in the book by Tapscott and Williams (2006), the data/information does not equal knowledge and, as the information becomes the headline of the new economy, and the world is sunken in an ocean of unsorted media impulses, the exclusive and relevant knowledge is the one which becomes more and more valuable. The problem of the knowledge security becomes more and more complicated also due to other aspects. First of all, knowledge security is mainly a human problem and not a technical one, being difficult to manage due to this reason. Secondly, more and more people state that the protection mechanisms used for traditional resources are not efficient in the case of knowledge, because an extreme security encumbers creativity, evolution and innovation. Cooperation and connection with the regional knowledge and talent sources worldwide, rather than the restriction of access to them, seem to be nowadays the foundation for the progress of organizations. Due to these reasons, we consider useful reassessing the knowledge security concept as regards the necessity of the innovation, which is in the agenda of any organization, and we will try in the current paper to find the most favorable ratio between openness and protection in the case knowledge.

The relevance of the confidentiality – integrity – accessibility triad into the knowledge security

For the beginning, we will bring forward the opportunity of using the traditional desiderates of the information security – confidentiality, integrity and accessibility, in the case of knowledge security.
The *confidentiality* of data and information is materialized in offering access to them only for authorized persons. Some of the most common security measures used in keeping confidentiality are the following: data and information are classified according to their importance (measured as the impact that information disclosure has on the organization), on several levels – that vary from public to top secret; employees are given authorizations and access rights according to the nature of their job, competences, the level of classification of the data and information they work with; the laws in force specific to the organization's field of activity (for example, the law on commercial secrets) are applied; confidentiality contracts are signed, they use passwords, encryption techniques, locks and keys, as well as safes.

Data and information *integrity* means that they must be kept in the correct and complete form and must not be modified without an authorization, either accidentally or on purpose. Among the measures for keeping the data and information integrity we mention here the mechanisms for checking the data in order to prevent errors from happening, back-ups, access control, training of the employees etc.

Accessibility refers to assuring the access to data and information, for authorized users, at any time. The well functioning of the hardware equipment and of the networks, back-ups, observance of laws etc., all these lead to this characteristic.

Starting from the observation of Randeree (2006), that firms with exclusive access to the knowledge resources gives them an advantage over competitors, we assume that confidentiality is also relevant in knowledge security. The annotation we bring is related to the tacit character of knowledge, which causes a new paradox: on the one hand, the easiest knowledge to secure is that which remains in the tacit form, as Bloodgood and Salisbury (2001) observed, and, on the other hand, taking into consideration the fact that the exclusive depositaries of tacit knowledge are the employees, their leaving the company can result in an important loss of valuable knowledge that has not been changed in due time from tacit knowledge into explicit knowledge. For example, we know that the absorptive capacity and the learning capacity of the firm are critical to the exploitation of knowledge resources – nevertheless, these abilities have a tacit character and are difficult to secure using the above-mentioned traditional methods. The security measures that can be applied to data and information in order to keep them confidential were built starting from their explicit character and can be used for explicit knowledge, but they must be reassessed in the case of tacit knowledge. The inadequate protection of knowledge may inhibit the transfer and sharing processes, as Damm and Schindler (2002) observed, and this fact has negative consequences on company innovation. In Julia Ryan's impressive words, "a world in which innovators can be held hostage due to poor security does little good for any of us. A world in which innovators can safely innovate while understanding the security challenges and managing them appropriately helps that rising tide lift all the boats. And we all win." And yet, "it simply is not reasonable to lock everything down, stop all communications, and limit employee access to the least amount of data necessary to perform their tasks. This would hinder efficiency, kill innovation, and massacre employee morale." (Ryan, 2006)

Regarding integrity, in the case of tacit knowledge we should also consider the dependence of this parameter to the employees' actions – for example, an employee leaving the company can result in an important loss of integrity, even when the employee does not affect the knowledge confidentiality, not revealing it whatsoever. The problem is related to the character of the tacit knowledge base that cannot be stored, unlike the data and information bases, as well as to the importance of the relational capital of an employee within a company – in other words, an employee leaving a team can make that team become unbalanced or even disappear. The protection measures must focus on the employee again, managers must do their best to draw the valuable knowledge from employees and store it on other environments that are easier to manage.

Knowledge accessibility is more and more often mentioned as an essential aspect in the innovative processes. Two of the preachers of the openness and cooperation based on shared knowledge are Don Tapscott and Anthony Williams (2006), according to whom public knowledge, capacity and resources incorporated into extended horizontal networks of participants, can be mobilized in order to obtain many more things than a company that acts on its own, whereas shut-in hierarchic corporations, that were once innovating secretly, can now participate and contribute to a global pool of talents – one that opens the knowledge workers world to any organization in search for a uniquely qualified mind to solve a problem. In this context, the communication of the corporations' information and knowledge that was previously considered a secret, to partners, employees, customers, stakeholders, as well to other groups interested in them, is becoming very important, and accessibility changes to transparency – offering adequate information and knowledge is a growing force in an economy connected to a network.

Therefore, we can assume that there is an inversion of the preoccupations regarding the guarantee of the knowledge confidentiality, integrity and accessibility as compared to the similar preoccupation for data and information, knowledge accessibility becoming, in the collaborative world nowadays, more important than their secret character – see figure no. 1.

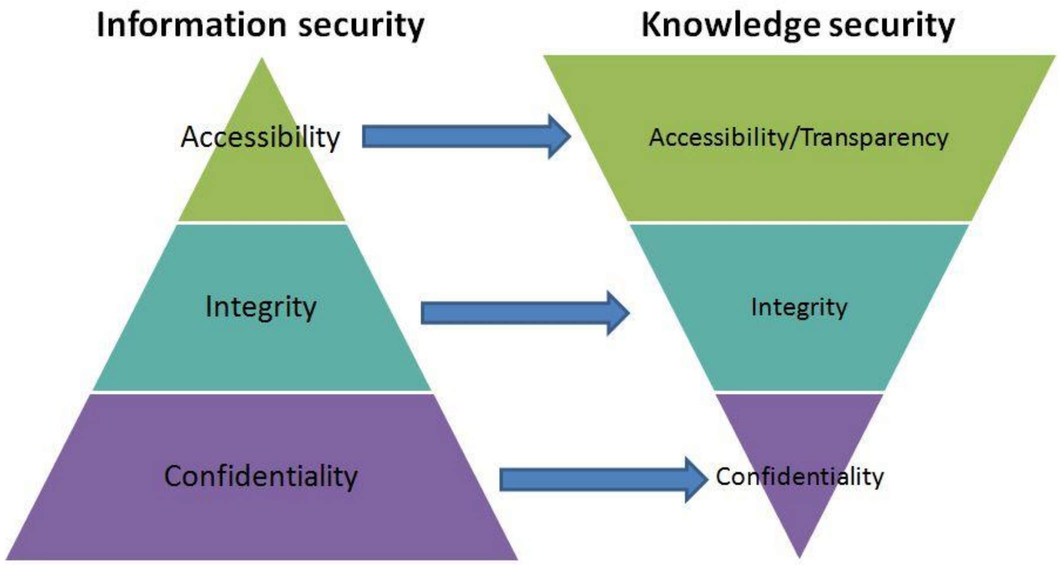

Fig 1. The CIA ratio inversion in the case of knowledge security

Some threats for organizational knowledge confidentiality, integrity and accessibility

Since we presume that, in the case of knowledge expressed and stored on various types of computer support and in various IT applications, the same IT security measures are applied as for data and information, we are going to analyze the characteristics of the great knowledge depositaries in an organization – the so-called knowledge workers, trying to identify the risks related to these characteristics. We are going to treat the risks according to the three above-mentioned major desiderates of any organization's security – confidentiality, integrity, accessibility.

The main characteristic of the knowledge workers is *the ability to delegate a part of their tasks to the technological applications and to adapt them to the business context*. Not having the normal, repetitive responsibilities, employees can use their time and efforts in *value-generating activities*, which require creativity and innovation. On the other side, the habit to use IT applications to fulfill their work tasks makes knowledge workers rapidly adopt new IT applications such as the social media. If in the company there are security measures of the applications implemented according to the organization's security policies, the security of new and appealing social networking and blogging applications raises serious problems for the general managers. A Recommind study published by Clifton in the May 2010 edition of the *InsideKnowledge* shows, somehow paradoxically, that many managers are worried regarding the risks associated to the use of the social media rather than the risks related to other new technologies, such as cloud computing. The attraction social networks have on people resides in their nature and in the way they store information – in conversations and connections rather than in highly structured and formalized databases and repositories. In this friendly and easy-to-accept environment, built in such a way so as to easily capture unstructured information and knowledge from various experiences, knowledge workers can unwillingly reveal sensitive elements about the company, thus affecting confidentiality. Web 2.0 combined with the contemporary "work-from-anywhere" lifestyle has begun to blur the lines between work and private life. Because of this psychological shift, people may inadvertently share knowledge their employer would have considered sensitive. Even if individuals aren't sharing the equivalent of trade secrets, the accumulation of the small "non-sensitive" items they share can allow a business's competitors to gain intelligence about what's going on and being worked on at that company, as mentioned in a study by Perez (2009).

Knowledge workers also have *an overall vision of the entire business* and *can determine exactly the place their activity has in meeting the organization's objectives.* Their abstracting capacity (understanding of the business strategies, of the company's organization and of the production processes) and their communication capacity (with the work teams, with customers) are of utmost importance. This new power given to the employees by the modification of their work tasks and the increase in the knowledge level necessary to perform these tasks made employees aware of the vital role they have within an organization. Combined with the *lack of loyalty*, more and more visible in the nowadays culture, the key position of the employees and the huge quantity of knowledge they have access to can be a potential danger regarding confidentiality (knowledge can be revealed to or made available for the competitors), integrity (employees can leave the firm taking the knowledge with them – especially the tacit knowledge captured in the organization) and accessibility (the employee does not wish to share knowledge).

Knowledge workers should also have the possibility to control and assess themselves, to learn by them continuously – in other words, they should be able to behave in an entrepreneurial manner, which involves a *high degree of responsibility and authority*. All employees should be able to assess the risks related to every action they perform, to communicate it to and analyze it with the team, thus observing the policies and avoiding the lack of involvement. Their autonomy is necessary since their tasks are much more complex and require a bigger effort as compared to the normal employees. Nevertheless, at the opposite end would be the possibility of the knowledge workers to leave the company earlier, not depending essentially on the organization they are working in. Since knowledge workers change their work place, they often keep informal relations with former colleagues – a research study by Dahl and Pendersen (2003) shows that employees with various levels of competences and positions within a company are prone to reveal their knowledge, knowledge that could sometimes endanger the company. Other categories of persons employees stay in touch with are the former university colleagues, as well as the members of the project team they were part of. Knowledge integrity is also extremely affected when valuable employees leave the organization.

Moreover, *the learning process of the knowledge workers is nowadays a life-long learning process*, as opposed to the manner in which people were trained up to now (for a single task, many times having a repetitive character, which was not modified very quickly). This evolution also changed the nature of families, which initially identified themselves with the work they did. The family model is changing – from the family where only one member was working, supporting the other members (giving up euphemisms, by "other members" we mean the wife and children) to a family in which both parents work. In order for the human and employee's rights to be observed and in order to synchronize the necessities of this family type with the work responsibilities, organizations became much more flexible, accepting forms such as part-time, permissive and variable schedules, parental leaves, a reduced work week length, flexible payment and contracts. This characteristic has an impact both on the confidentiality and on the integrity of the knowledge used in various environments, much more insecure comparing to the rigid context of the organization – the mail box accessed from the Blackberry or from the laptop is a significant example of knowledge insecurity. Many employees' desire to keep control over their own position even when they are on holiday also exposes the company to the risks of using knowledge outside its area. A research commissioned by Credant Technologies and mentioned in Clifton (2010) found that 64 percent of the respondents were travelling with their laptops. 66 percent of these machines were unencrypted and 51 percent were totally insecure, without as much as a password for added protection.

Knowledge workers are *much more educated*. Foreign languages and the ICT competences are vital for a career in almost any field, and, at the same time, mastered by more and more people. Dissolution of the "professions" as they are understood nowadays is likely to take place in the future, each knowledge worker having a multivalent and multi-disciplinary education. Strict, high-level knowledge, characteristic to a narrow area of activity (many times explicit and coded), will be exceeded by characteristics such as flexibility, creativity and adaptability (which most of the times will either generate or use implicit knowledge). Organizations should use the benefits of this new situation and treat their employees as an endless source of ideas and analytical thinking. The amendment we would like to bring to this positive feature of the contemporary employees is due to the difficulty to transmit and reuse this knowledge in the organization. This phenomenon which is difficult to measure and manage does not appear in the case of data and information accessibility – computers do not need flattery and encouragement in order to facilitate the transfer of and access to information. As specified by Collison (2010), people do not share knowledge (lessons, good practices) for fear not to be replaced by others (the "tall poppy syndrome") or because they consider they do not have anything important to say ("shrinking violet"). The crisis and uncertainty regarding the day of tomorrow increase people's tendency not to reveal their knowledge. "What I know determines my value" is preferred instead of "my ability to quickly learn, grow and adapt determines my value" – and therefore the animosity regarding knowledge transfer.

Recommended knowledge security measures

Regarding the proper measures for guaranteeing knowledge security, we think that managers should bear in mind that the employee should be at the center of the preoccupations for the knowledge security. If elements such as the ones mentioned below are introduced in the management activity, knowledge security will appear naturally, as an emerging opportunity of the actions of every single individual.

Acknowledgement - Managers and employees should acknowledge the lack of correspondence between the data and information security and knowledge security. Even if the technological equipment used for the storage of knowledge is as safe as the one used for data and information, people who administer the content must be ready to use the system adequately and to store various types of knowledge. The IT, legal and risk departments should cooperate and their actions should be correlated. Managers and employees should acknowledge the fact that knowledge security involves all three aspects mentioned above – confidentiality, integrity and accessibility.

Training - Employees' training regarding the necessity of the security of knowledge they work with. The training can be done either by consultants experts (usually treated more seriously by employees and by the organization – which pays them and expects results) or by employees, by training sessions or even informal meetings based on stories, happenings, ways to transfer knowledge as naturally as can be.

Motivation - From the very beginning, teams or organizations should hunt positive people, willing to get involved, whereas those who want to be stars will be left aside. Motivation, staff involvement – besides the traditional stimuli, such as salary or a rapid promotion – a positive attitude of managers and a pleasant working environment are also desirable.

Concrete measures - Stipulation of competition clauses in knowledge worker's contracts, used as proxy for a firm's actions towards limiting the disclosure of knowledge to other firms through informal channels.

Attitude - Employees should receive the same respect and responsibility employers offer experts. People's safety that the organization will not get rid of them, the transparency in using knowledge and the desire to improve the environment should be increased - using instruments such as the peer assist, communities of practices, offers and requests, self-assessment and internal benchmarking, river diagrams and knowledge cafes. Social media is a solution because it covers the traditional hierarchy structures and increases participation. Besides the techniques, the visible involvement of the leader is the one that makes the difference. At the same time, managers must encourage the knowledge requirement aspect, because people are normally
1) reserved regarding ideas or good practices which come from outside the organization or from one of its different areas,
2) self-sufficient, that is, they avoid requiring somebody else's help in order not to seem weak. Solutions to encourage the requirement are knowledge fairs, internal benchmarking, and communities of practice.

The correct treatment – the violation of a correct process logically involves the non-recognition of the individuals' intellectual and emotional value. The well-known thought and behavior pattern in this case can be summarized as follows: if individuals are not treated as if their knowledge mattered, they will feel intellectually indignated and will not share their ideas and experience; they will rather keep the most logical reasoning and the most creative ideas for themselves, not allowing new perspectives to come into the light. Moreover, they will deny other employees' intellectual value. It is as if they said: "You don't appreciate my ideas, I won't appreciate yours. I don't even trust and care about the strategic decisions you made", as Chan Kim and Mauborgne (2007) observed.

The focus on the relationship among data, information and knowledge, and not only on the "end products" – Bard and Söderqvist (2002) mentioned that the theoretical separation that literature does among data, information and knowledge can be helpful for managers that can better understand the nature of the informational conglomerate they deal with in their daily activity and each employee's role in the production of valuable informational assets for the company, especially if the central value of the informational economy is not the information itself, but the information sorting and combination, processes that cannot be protected by copyrights, firewalls or encryption. The responsibility of a knowledge manager is not to manage information and knowledge, but rather to manage the relationships that influence the way in which information is divided, the way in which divided information becomes (and generates) knowledge, how to manage the combination between relationships, knowledge and information for a large variety of organizational purposes.

Communication – over communication can harm love relationships, but when it comes to business relationships, the managers should consider all the ways in which communication works (either electronically or face to face). An important challenge is to *effectively* communicate vision, rules, and guidelines to employees and other stakeholders. Currently, security policies are used for this purpose. However, as Belsis et al (2005) observed, policies are static documents that reflect the technical and organizational context at the time of their creation.

Conclusion

Nowadays, the informational work market has a completely new structure. Jobs are no longer a life-long contract, and seniority is not so important. Organizations become less rigid and focus on temporary projects, for which they hire people with certain competences. Constellations are created but they disappear when the project has finished. Education is a developing process that needs to be updated on a daily basis. Every new task involves a new situation that usually requires new knowledge. Employees, as depositaries and creators of knowledge, become the organization's most valuable elements. The intensification of their activity in such a way so as to use a higher volume of the stored and generated knowledge to the benefit of the company is a crucial element. Unfortunately, unlike the data and information security, there is no steady network that managers can use for the knowledge security.

As a conclusion, we bring to the auditors' attention a quotation that belongs to Brian Eno: *Control and surrender have to be kept in balance. That's what surfers do – take control of the situation, then be carried, then take control. In the last few thousand years, we've become incredibly adept technically. We've treasured the controlling part of ourselves and neglected the surrendering part.* Starting from this quotation and taking into account the flakiness of the resource discussed in the paper – we recommend managers to balance the security measures and the staff degree of freedom, taking into account that, as Ward (2010) said, the knowledge management – the best of it – consists in the effort to make something so that the untouchable, hard-to-get, personified parts of the knowledge, values, history, culture and experience of an organization to get to the surface, becoming accessible and expressible, without endangering its position on the market and innovation capability.

Acknowledgement

This paper received financial support through the project *SPODE - Postdoctoral Studies in Economics: training program for elite researchers* (contract no. POSDRU/ 89/1.5/S/61755, Human Resources Development Operational Programme 2007-2013 funded by European Social Fund).

References:

Bard, A., Söderqvist, J. (2002), Netocracy: the new power elite and life after capitalism, BookHouse Publishing AB, Stockholm

Belsis, P., Kokolakis, S. and Kiountouzis, E. (2005), "Information systems security from a knowledge management perspective", *Information Management & Computer Security Journal*, Volume 13, Number 3, 2005, pp. 189-202, Emerald Group Publishing Limited

Bloodgood, J.M. and Salisbury, W.D. (2001), "Understanding the influence of organizational change strategies on information technology and knowledge management strategies", *Decision Support Systems*, Vol. 31 No. 1, pp. 55-69

Chan Kim, W., Mauborgne, R. (2007), Strategia oceanului albastru, Ed. Curtea Veche, Bucureşti, p. 240

Clifton, K. (2010), "From the editor", *Inside Knowledge*, Vol. 13, Issue 8, p. 3

Collison, C. (2010), "Flower power", *Inside Knowledge*, May 2010, Vol. 13, Issue 8, p. 11

Dahl, M. and Pendersen, C. (2003), "Knowledge Flows through Informal Contacts in Industrial Clusters: Myths or Realities?", DRUID Working Paper No 03-01, [Online] [Retreived March 17, 2011] Available: http:/v/ideas.repec.org/p/aal/abbswp/03-01.html

Damm, D. and Schindler, M. (2002), "Security issues of a knowledge medium for distributed project work", *International Journal of Project Management*, Vol. 20 No. 1, pp. 37-47

Delgado-Verde, M., Martin-de Castro, G. and Navas-Lopez, J. E. (2011), "Organizational knowledge assets and innovation capability. Evidence from Spanish manufacturing firms", *Journal of Intellectual Capital*, Vol. 12 No. 1, pp. 5-19, Emerald Group Publishing Limited

Fotache, M. (2002), "Probleme generale ale managementului cunoştinţelor (General Aspects of Knowledge Management)", FEAA [Online], [Retrieved March 12, 2011], http:// www.feaa.uaic.ro/cercetare/simpozioane/24_26_ oct_2002/ziua2/sectiunea_II/PROBLEME%20GENERALE%20ALE%20MANAGEMENTULUI%20CUNOSTINTELOR.pdf

Jeffries, S. (2010), "Surrender. It's Brian Eno" [Online], [Retrieved March 12, 2011], http://www.guardian. co.uk/music/2010/apr/28/brian-eno-brighton-festival quoted in Ward, V., *Inside Knowledge*, May 2010, Vol. 13, Issue 8, p. 6

Perez, S. (February 17 2009), "Top 8 Web 2.0 Security Threats", [Online] [Retrieved March 13 2011], http://www.readwriteweb.com/enterprise/2009/02/top-8-web-20-security-threats.php.

Peri, G. (2002), "Knowledge Flows And Innovation", [Online] [Retrieved March 18 2011], http://elsa.berkeley.edu/~obstfeld/e281_sp03/peri.pdf

Randeree, E. (2006), "Knowledge management: securing the future", *Journal of Knowledge Management*, Vol. 10, No. 4, pp. 145-156, Emerald Group Publishing Limited

Ryan, J. (2006), "Knowledge management needs security too", *VINE: The Journal of Information and Knowledge Management Systems*, Volume 36, No. 1, pp. 45-48, Emerald Group Publishing Limited

Ryan, J. (2006), "Managing knowledge security", *VINE: The Journal of Information and Knowledge Management Systems*, Vol. 36, No. 2, 2006, pp. 143-145, Emerald Group Publishing Limited

Tapscott, D., Williams, A. (2006), Wikinomics, Portfolio/Penguin, Penguin Group, New York

Tapscott, D., Williams, A. (2010), Macrowikinomics, Portfolio/Penguin, Penguin Group, New York

Ward, V. (2010), ***, *Inside Knowledge*, Vol. 13, Issue 8, p. 5