



TLO
12,2

Managing corporate risk through better knowledge management

Dale Neef

Chester, New Jersey, USA

112

Abstract

Purpose – To explain how progressive companies are using a combination of knowledge and risk management (KRM) systems and techniques in order to help them to prevent, or respond most effectively to, ethical or reputation-damaging incidents.

Design/methodology/approach – The paper explains KRM, develops a corporate integrity framework, and then explores how the KRM process component of the framework is related to the use of knowledge management (KM)-related procedures, techniques, and tools in use in many corporations.

Findings – In many forward-looking corporations KM procedures, techniques and tools are being used to perform risk management. KRM, the integration of knowledge and risk management, is alive and well and, given the global importance of risk management, may provide KM with a much-needed and revitalizing boost.

Originality/value – The value of the KRM perspective is its development of a new and comprehensive application of KM to the vital global corporate need of risk management.

Keywords Knowledge management, Risk management, Social responsibility, Corporate strategy

Paper type General review

Introduction

Some contend that knowledge management has already “been done”, and that further elaboration of its benefits and continued advocacy for expanding its application within the modern organization is *passé*. However, in an era of corporate scandal and expanding global supply chains, knowledge management is witnessing a renaissance as a key tool for managing corporate risk. In fact, far from being “done”, in many ways it is only now, when effective risk and incident management has become so integral to corporate well-being, that knowledge management has truly become a mainstream and strategic management tool. This is simply because a company cannot manage its risk effectively if it cannot manage its knowledge.

A quick review of the relationship between risk and knowledge management makes it clear why this renewed interest in knowledge management tools and techniques is so important. Consider, for example: a 16-month old child dies from drinking bacteria-laden apple juice after the company ignores advice concerning the product’s safety. A slaughterhouse finds its employees dumping waste chicken blood and entrails into one of Mississippi’s main water systems. A children’s safety seat manufacturer fails to reveal to the public dangerous defects in its car seats, cribs and strollers that kill two babies and injure more than 300 others.

What do these types of unethical and illegal corporate behavior have to do with knowledge management?

This article is loosely excerpted from Neef (2003).



The answer is “everything”, because (putting aside some obvious cases of pure malfeasance on the part of corporate executives in recent scandals), most reputation-damaging incidents that occur today are often less a question of a lapse in ethical policy than they are a colossal failure on the part of company decision makers, corporate officers, and board members, to manage corporate knowledge and risk. After all, most corporate disasters – a product safety violation, employing under-aged workers, or illegal disposal of wastes – are not the sort of thing that company executives or board members would normally endorse. The reason most often cited when these disastrous incidents occur (these days, quite often in front of a judge) is that senior company leaders had no knowledge of what was taking place in their company. Furthermore, sadly, very often their claims of complete ignorance seem to be true.

Risk management *is* knowledge management

For a growing number of knowledge and risk management experts, the fact that corporate leaders remain ignorant about harmful, illegal, or reputation-threatening activities within their own organizations provides the most compelling case yet for better knowledge management in the modern company. After all, many of the issues that organizational leaders complain prevent them from anticipating and reacting to a corporate ethical crises, are the same issues that knowledge management experts (see for example, Nonaka and Takeuchi, 1995; Ashkenas, 1995; Chawla and Renesch, 1994) have been wrestling with for years.

The rationale for applying these knowledge management techniques and systems to a broader corporate ethics and risk program is straightforward:

- Sensing and responding to risks in an organization is very much dependent on corporate intellectual capital – i.e. the knowledge and judgment of employees at all levels. Employee insight – in terms of anticipating potential accidents, a personal recollection from a similar incident in the past, a story swapped weeks ago around the coffee machine that can alert a supervisor to an impending manufacturing line accident or environmental spill – all can keep a disaster from occurring.
- However, that knowledge is much less effective if left to filter through a management structure in a haphazard way. It needs to be actively managed and encouraged, so that employees see concern for ethical or legal violations as part of their everyday responsibility.
- Accordingly, key company decision makers need to mobilize this employee knowledge and the vast amount of information available concerning potentially reputation-threatening issues in a way that will allow them to “sense and respond” quickly and correctly to developing risks. To do this they will need to monitor ethical sourcing activities of overseas suppliers, as well as local, political, cultural, economic, and environmental issues so that potentially explosive issues can quickly be brought to the attention of a “crisis team” and prevented or resolved.
- Companies need to create objective, scenario-based guidelines for ethical behavior, communicating those guidelines among key organizational leaders, and providing a workable system of incentives for managers to help them

encourage employees to uncover potentially dangerous issues. This will involve knowledge management techniques concerned with opening communication channels – both human and electronic – so that executives can communicate a corporate policy of integrity to their employees with specific guidelines that go well beyond the (often banal) vision-level integrity statements that so many companies now employ.

- Finally, once resolved, organizations need to capture “lessons learned”, apply proven risk management techniques, and create decision support systems that will help the organization to develop preventive risk management policies and avoid costly repetition of errors. Neef (2003) develops the rationale for this point in much greater detail.

In short, the key to a proactive risk management process lies in the company’s ability to mobilize the knowledge and expertise of its employees so that organizational leaders can ensure that they get accurate and timely information about a potentially harmful incident. In fact, many experts agree that “an organization can’t manage its risk today without managing its knowledge” (Lelic, 2002).

This realization has spawned a new movement, known as integrated knowledge and risk management (KRM), which is possibly one of the most important steps in the evolution of the modern corporation since business process reengineering more than 15 years ago.

Applying knowledge management to a corporate ethics and risk management strategy

The good news is that adopting a strategic approach to KRM is neither exceptionally expensive nor particularly difficult. The internet and supporting IT technologies, for example, give company planners access to unprecedented high-quality information regarding new legislation or scientific, cultural, political or economic issues that might affect the organization. Companies can turn to accurate market analysis tools to understand potential market risks, (Leonard-Barton, 1995, p. 135) and have instant access to journals, newswires, and complex and specialized business research and analysis systems (Davenport, 1995). Safety and incident management applications can present senior management with accurate reports on safety violations (Kartalia, 2000), identifying trends that can reveal potentially damaging risks to come. In terms of new knowledge management techniques and information access, companies have never had it so good.

Moreover, most of these techniques, processes and systems exist – or should exist – already in the modern company. Enterprise resource planning systems provide key company-wide performance data, and environmental health and safety systems can record trends and provide early alert and incident management techniques (Neef, 2003, Ch. 10). Knowledge management tools – e-mail, the internet, early alert teams, (Marquardt, 1994, p. 41) communities of practice, capturing and distributing “lessons learned” – can all be applied in a formal process that will help a company to sense and respond to potential risks.

In fact, despite the increased risk to a corporation’s reputation that comes with the new global environment, with all the advancements in IT, process, and management techniques made in the past two decades, companies have very little excuse for

continuing to take a drubbing because of costly and predictable mistakes when it comes to corporate integrity issues. However, all of this means re-thinking the way that the organization approaches the issues of KRM, setting up an ethical framework as a company, and reorganizing systems and processes specifically to focus on preventing ethical disasters (Neef, 2003).

The bad news, however, is that, despite the near universal availability of these tools and practices, few companies have actually attempted to integrate these systems into a formal process of KRM (Neef, 2003). Even for companies that have adopted knowledge management processes and systems over the past several years, too often these remain almost exclusively focused on coordinating operational knowledge and increasing productivity, and not on identifying and managing potential risks (Neef, 2003).

A recent KPMG survey of 35 companies with revenues of \$500 million or more, for example, found that 47 percent of those companies had no crisis preparedness plan in place, even though 81 percent said they thought their companies were vulnerable to a serious operational incident (Taub, 2002). Even fewer organizations have any formal framework for identifying, assessing and dealing with risk. In reality, despite the KRM tools at their disposal, most companies remain, more or less, in the same mindset that they have been in for the past century when it comes to integrity and risk management.

Key elements of the modern ethical framework

Fortunately, there are an increasing number of progressive corporations that are effectively applying KRM techniques to avoid operational and ethical disasters. Companies in the frontline of globalization, such as those in the petroleum, chemical, and apparel manufacturing industries, as well as those that have evolved under strict regulatory regimes – defense contractors and pharmaceuticals – are among the leaders in integrated ethics and risk management, and companies such as BAA, Intel, Novo Nordisk, and Nike have all developed strong new approaches to risk management, incorporating advanced ethical monitoring and reporting processes and systems based on knowledge management systems and techniques (Neef, 2003).

What are the key aspects of these companies' approach to KRM? There are four important areas of focus that leading companies incorporate into an integrated KRM program:

- (1) An organization needs a coordinated, well-managed program specifically focused on an ethical management framework. This framework usually consists of board and senior-level leadership, a dedicated ethics and risk management center of excellence, a chief ethics risk officer, a value statement, corporate conduct guidelines, and a dedicated and ethics-focused education and communication program supported by incentives and punishments.
- (2) Reflecting the adage that “you cannot manage what you cannot measure”, these companies have adopted international and auditable performance standards that provide new levels of due diligence concerning ethical, social, and environmental risk.
- (3) These organizations have adopted open, transparent, verifiable reporting on “softer” non-financial subjects using triple-bottom-line accounting (Elkington, 1998) and reporting techniques.

- (4) These companies are instituting an integrated KRM process. This means creating a dedicated knowledge management process that leverages best practice risk and knowledge management procedures and systems that reach from the shop floor to the board and senior company officers. Together these four key components make up a modern organization's integrity framework (see Figure 1).

Applying knowledge management procedures and techniques

Although each of these four areas are important, this paper will focus on the fourth component, the integrated KRM process; and possibly the best way to understand what is meant by knowledge management in the context of KRM and a corporate integrity framework is simply to look at some important knowledge management techniques and systems that are being used by these organizations. These include:

- (1) *Knowledge mapping*. Knowledge mapping is a process by which an organization determines "who knows what" in the company. It has many forms, including skills mapping, where employees list specialty knowledge and project experience, which is then captured in a relational database and made available through the company's knowledge management portal. Sometimes known as "knowledge yellow pages" (Davenport, 1998, p. 72), this skills and experience mapping allows a company to understand where experience and expertise lies in the company, and where needed skills or knowledge may be missing.

An extension of this idea is the use of an "accountability matrix" where those employees who are responsible for making decisions or supervising tasks are mapped and tied together electronically through a relational database and software application so that responsibility for project decisions – or advice on a developing crises – can instantly be assessed when an important decision needs to be made quickly.

- (2) "*Communities of practice*". Communities of practice are naturally-forming networks of employees with similar interests or experience, or with



Figure 1.
The corporate integrity
framework

complementary skills, who would normally gather to discuss common issues. In KRM, communities of practice are actively identified, and members of these networks are encouraged to gather and exchange ideas concerning potential ethical or reputation-threatening activities on a formal basis, capturing lessons learned, swapping ideas, and sharing insight. This formal management of what is usually an informal process helps an organization to create a company culture where knowledge sharing is encouraged, ethical behavior is actively rewarded, and opinions and ideas flow more freely among departments and offices.

In fact, most serious ethical incidents involve lower-level employees and can be prevented if detected early and brought through a formal process to executive decision makers or the board. However, this early detection is dependent on employees “on the ground” sensing and responding to early warning signs, that in their experience, indicate a potential incident. A company needs formally to create a process for communicating these values and encourage sharing of ideas and ethical concerns generally.

- (3) *“Hard-tagging” experts.* Hard tagging is a knowledge management process that combines knowledge mapping with a formal mentoring process. As part of the knowledge mapping and skills mapping process, experienced employees are identified or “hard tagged” so they will become part of a consultation pool that will be available when special advice is needed on developing incidents. These “hard tagged” specialists also team in communities of practice with “soft tagged” employees – those who are interested in learning specialist skills or in sharing experience – in a mentoring and knowledge sharing exercise (McGee and Prusak, 1993, Ch. 4).

Making information and experience available to company leaders during an incident or potential crisis is critical to the decision-making process of risk management, and decision making in an advanced risk management process should involve consultation with an incident management team, made up of experts from a community of practice or a knowledge network, who are best able to analyze, debate, and help agree on a course of action. The decision-making process, therefore, becomes much better informed and balanced, with contributions from people who understand the situation, from experts that have experience with similar events, from those who can advise on scenarios and plans for resolution, and from the decision makers themselves. Access and speed are often crucial to the success of incident management decision making, so electronic knowledge mapping is used to bring together critical information to team members, as well as to notify deputies in the event that a hard-tagged specialist is not immediately available.

- (4) *Learning.* One of the most important tenets of knowledge management is that employees should share experiences and techniques with others in the company so that there is a continuous and dynamic process of knowledge sharing and learning taking place. After event reviews, such as those used in the military and many leading companies these days, help specialists to debrief and “post-mortem” incidents – learning from both what they did right and what they did wrong in the situation.

One of the greatest benefits from this process of post-incident assessment and continuous learning is that employees digest “lessons learned” from previous

mistakes, and that problem resolution does not each time require “re-inventing the wheel”. The mentoring aspect of hard tagging, meetings within communities of practice, and formal exchange of “best practices” all contribute to not only a better informed workforce, but also retaining a “corporate memory”, so that incidents do not reoccur.

- (5) *Encouraging a knowledge-sharing culture.* Central to the success of a KRM framework, is the concept that values and expectations for ethical behavior need to be communicated widely and effectively throughout the organization. In short, integrity has to become part of the corporate culture. This is best accomplished as part of a formal process of knowledge sharing, of mentoring, and formal ethics training, so that employees at all levels appreciate the importance of good behavior. This means that there needs to be regular and consistent communication on values and on processes that encourage sharing of ideas and early identification of risks. This process of formal, company-advocated knowledge sharing sends the important message to employees throughout the organization that they have responsibility and authority to voice concerns and act on ethical, legal or safety issues that might harm the company.
- (6) *Performance monitoring and reporting.* Underlying a successful knowledge foundation is the need to measure, monitor, and boast of organizational performance. This has been part of the “measures that matter” movement that began in earnest with knowledge management several years ago, where non-financial performance information – including intellectual and organizational capital – is used to predict the future success of a company (Low and Kalafut, 2002). In keeping with the move toward greater transparency and better non-financial reporting, as part of their formal knowledge management process a company should use international standards and reporting guidelines to help measure and publish statistics on human, social, environmental and “integrity” performance.
- (7) *Community and stakeholder involvement.* Communication and knowledge sharing is key to good knowledge management. This holds true not only for a company’s employees, but also for the many stakeholders that are interested in company policy. Systems – e-mail, electronic newsletters, collaborative online project planning – can all help not only to keep stakeholders informed of company policy, but also to help company leaders sense and respond to early concerns from these outside parties (government, unions, non-governmental or activist groups, the press, etc.), on policy matters that could later develop into serious conflicts or incidents.
- (8) *Business research and analysis.* Finally, one of the most revolutionary and valuable features of knowledge management today is the ability of a company to gain access to enormous amounts of business research and analysis materials. As part of a knowledge and risk management process, companies need to create an information gathering capacity, developing a knowledge “research and analysis” capability in order to search for, organize and distribute information from internal and external sources concerning local political, cultural, and legal concerns. This should include the ability to complete formal research in areas such as:

- regulatory and legal policies;
- company violations and fines for non-compliance;
- local political, social, and regulatory climate in areas of new or potential project development;
- internet and press reports on the company's performance;
- social and environmental performance of subcontractors and their reputation in the local community; and
- capturing leading practice and lessons learned (both internal and among the competition).

KRM in practice

Intel provides a good example of how these techniques are being used to mediate risk.

Several years ago, the company put in place a global tracking system for managing the “top ten” issues emerging under corporate responsibility. This issue tracking system is based on a URL site that is available to all employees and addresses issues such as human resources, legal, community issues at production sites, corporate welfare, environmental health and safety, product impact, product ecology, the social aspects of their technology, investor relations, governmental affairs, market impacts, and political contributions.

Building on their long-standing “Right to Know” policy, the site is a source for questions or comments from employees anywhere in the world on these issues, and provides the company with important insight on emerging issues and risks, which are automatically directed to company experts and leaders. The site is also used to post answers to employee questions, to explain Intel policies, to provide relevant articles, and contact information on content owners and company experts. In addition, each week their corporate responsibility department provides more than 100 key experts in the company with a summarized newsletter on emerging issues. It is an effective two-way program of communication and issue identification and resolution.

KRM and technology

As the Intel example illustrates, there are also various software solutions that can be used to support these KRM techniques: to help identify experts, to collect and distribute important information, to capture lessons learned, and to complete business research and analysis. Possibly more important is that the communication and organizing features of the modern intranet, groupware and relational database technologies, need to be used to help capture, organize and distribute relevant and time-sensitive information about key performance areas, risks or opportunities to those who need it in a timely way.

This process needs, in turn, to be coordinated utilizing information management rules concerning priority and timeliness in order to overcome the massive “information overload” that can mean critical risk information is never acted on or lost among hundreds of e-mails or project updates.

So what are some of these technologies?

The internet, the web and a company's intranet

The most valuable knowledge management information technology tool may well be the software that is now universal in all companies – e-mail and groupware, and access to the world wide web via the internet. These systems can today provide most of the important functions that are required for ongoing knowledge management tasks, providing a secure network for communication, data collection and storage. The standard features of these systems – groupware, e-mail, search engines, shared applications, document storage and common retrieval functionality – all help employees to work collaboratively in virtual teams, regardless of their geography. Moreover, access to the internet through browsers and search engines can provide employees with information on political, legislative, and commercial issues, or best practice techniques.

And, of course, the company intranet is an effective way of communicating standard operating procedures, risk management objectives and ethical policy to both employees and suppliers, or for contacting and briefing members of the hard-tagged knowledge network when an incident arises. This versatile framework also provides the integral system logic for mapping, indexing, relating and finding information through browsers and search engines that is so crucial to the knowledge management process.

Knowledge management systems

There are also a number of more specific knowledge management software applications that can provide a company with special functionality that can be used as part of a KRM platform, including:

- Specialized search tools that allow employees throughout the company to quickly find documented information not only on the internet, but particularly in company databases and repositories.
- External business research and analysis and reputation management tools, including specialist databases for subjects or industries, access to professional research and industry reports, and contacts with global specialists outside the company.
- Knowledge mapping tools that provide skills databases and knowledge mapping functions, as well as tools that can identify company employees with similar or recent incident experience, or certification and training in specialist areas. These tools can complete a knowledge gap analysis for defining education and training needs, and can also provide a useful escalation process so that a priority query is instantly distributed to a group of experts and company executives to ensure a rapid response.
- Collaboration tools for online collaboration during an early alert team or incident investigation, or when drawing in opinions from “hard tagged” specialists scattered around the company. These systems include mechanisms for simultaneous screen viewing and live online conversations.
- Capturing leading practice and lessons learned: template-based tools that make it easy for employees to input key lessons learned in a standardized format to a central repository.

- Administrative tools for measuring system usage and tracking trends allow knowledge management specialists to monitor and “tune” systems depending on need, effectiveness, and usage statistics.
- Records retention tools – document organization and retention policies remain at the heart of an effective KRM process. There are countless stories of executives explaining that the key information that could have helped to alert them to potential risks – missed maintenance activities, illegal storage of toxic substances, health inspection warnings, emissions violations – was simply lost, or at least never captured, in the information jungle.

The sheer volume of information that is created everyday within the modern company means that an organization needs an effective way of deciding what information to destroy, what to retain, and how to organize that which remains for easy retrieval. This is particularly true when investigating a particular risk area, or when an incident has developed into legal action that may require extra care in information collection. Any event that is likely to lead to an investigation or require a detailed explanation of what the company knew, when, and what they did in response, will require an effective system of document retention and retrieval (Neef, 2003, Ch.10).

Environmental management information systems and integrated risk management software

Finally, environmental management information systems (EMIS) are, in terms of ethics and risk management, one of the more important suites of software tools that have emerged in the past several years (Neef, 2003, Ch. 10). These systems usually provide a variety of important environmental tracking and performance tools, including legislative change notifications, and flexible report generators for tracking of a company’s performance – or non-conformance – set against state and federal environmental (and sometimes health and safety) requirements. Most systems also provide tools that help a company to track energy usage, recycling efforts, and emissions, so that they can monitor costs and create efficiencies where possible. Although separate from formal KRM systems, they can be used to augment the techniques and systems already described, and are quickly becoming integral to the KRM process.

This is in part because recently these EMIS have begun to expand to take on many of the features of a fuller risk management system, providing additional functionality that goes beyond just resource or energy compliance and efficiency monitoring. In keeping with the emerging requirements for ethical, social, and environmental corporate reporting, several progressive software companies (Neef, 2003, Ch. 10) now provide modules for measuring, managing and reporting on other issues such as employment rights performance, and even corporate governance standards.

These robust, integrated, enterprise-wide risk management systems can provide not only access to a central repository of all risk management-related documents, but also tools for mapping, ranking and tracking risks, identifying stakeholders and specialists, and monitoring the steps being taken to contain the risk. These systems can even be proactive and dynamic, helping to provide early warning of developing issues and alerting those responsible for managing risks in a particular area. These systems usually have several key features:

- (1) *Communications functions.* One of the key features of any enterprise system is its ability to communicate broadly with employees and stakeholders. Most EMIS provide various links to company news, to legislative changes, or to changes to company policies and programs on the organization's intranet site or portal. These tools make it easy for employees to locate standard operating procedures and leading practice guidelines, and can also be used to post press reports, or company position statements on issues or incidents. Most suites also provide a "chat page" forum specifically allocated to issues of ethics and risk, which can be invaluable as part of a way to identify potential issues from employees anywhere in the company, worldwide.
- (2) *Risk management functions.* Enterprise risk management software platforms usually also provide a variety of day-to-day risk management tools. These include:
 - audit and non-conformance alerts, which means that issues are immediately flagged for action and can be monitored through resolution by those in various departments or management ranks;
 - customizable risk "mapping" tools for deciding what issues need to be monitored, allowing process owners to identify and map risks in their responsibility areas;
 - tools that help management to set and monitor individual and unit key performance indicators;
 - various features for day-to-day management of compliance reporting, including a complete submission history of documentation, pre-formatted OSHA and EHS forms, and prompts for follow-up documentation; and
 - a searchable, relational database and repository for all risk-related information.
- (3) *Incident management tools.* Once an incident has happened, organizations need to have a means for specifically tracking, managing, and resolving the situation. These tools provide all the relevant information to various parties involved with a particular incident automatically and consistently, and act as a repository for the complete record of events from investigation to close. They help to collect relevant information, including:
 - a description of the circumstances;
 - employees involved;
 - assets, projects or departments involved or affected;
 - resources needed for resolution;
 - possible repercussions;
 - likely costs;
 - actions taken; and
 - resolution activities and closing audits.

They also guide a company through the steps necessary to manage resolution, including a responsibility matrix that identifies and contacts key decision

makers in the incident resolution process, and a “contact manager” feature for identifying and contacting hard-tagged experts, both within the company and among outside experts.

- (4) *Decision-support tools.* One of the greatest challenges for the modern company is being able to take advantage of all the information collection possibilities that exist with new technologies – information on internal operations, on current emissions policies, on safety violations, or concerns raised by employees – and to manage and interpret all of this information in a way that is of value to many different groups within the company.

Decision-support tools help to filter and prioritize information from various sources – EHS or CRM systems, e-mails, incident management systems, or strategic (procurement) sourcing software – and to manipulate the data in different ways in order to perform risk analysis, risk prioritization and “what if” scenario planning. These tools can be set to focus on key environmental, financial or social performance indicators, and can provide benchmark comparisons between different factories, facilities, and suppliers.

- (5) *Reporting tools.* Finally, one of the most important features of these systems is their ability to produce customizable reports for the various parties involved in the KRM process - risk managers, operational process owners, management or board members. These tools can be configured to use relevant information, and combine various display formats, graphs and diagrams (Neef, 2003, Ch. 10).

Conclusion

What is important to realize, as most readers no doubt have, is that the types of activities that have been described in this article, and the systems, infrastructure and processes that support them, are not so different from what many knowledge management strategists have been advocating for years. That is why many organizations, such as BT, Intel or ChevronTexaco, are today integrating and coordinating their existing safety, supply chain and knowledge management systems in a more coordinated way, as part of a broader risk management program.

There are many benefits from actively managing the knowledge of an organization, and the practice of knowledge management has advanced far in its thinking – from soft to tangible – in the past several years. Far from being *passé*, the fact that those same systems and techniques are now being used by organizations as part of a broader ethical and risk management framework helps to make knowledge management practices at once more mainstream and more easily explained to skeptics and the uninitiated. In fact, given the importance of risk management in the global economy (and given there can be no risk management without good knowledge management), KRM may provide the knowledge management movement with a much-needed and revitalizing boost.

References

- Ashkenas, R. (1995), *The Boundaryless Organization*, Jossey-Bass, San Francisco, CA.
Chawla, S. and Renesch, J. (Eds) (1994), *Learning Organizations*, Productivity Press, Portland, OR.

- Davenport, T. (1995), *Information Ecology*, Oxford University Press, New York, NY.
- Davenport, T. (1998), *Working Knowledge*, Harvard Business School Press, Boston, MA.
- Elkington, J. (1998), *Cannibals with Forks: The Triple Bottom Line of 21st Century Business (Conscientious Commerce)*, New Society Publishers, Gabriola Island.
- Kartalia, J. (2000), "Reputation at risk?", *Risk Management*, May, available at: www.rims.org/mmag
- Lelic, S. (2002), "Managing knowledge to manage risk", *Knowledge Management*, Vol. 6 No. 1, September 2, available at: www.kmmagazine.com
- Leonard-Barton, D. (1995), *Wellsprings of Knowledge*, Harvard Business School Press, Boston, MA.
- Low, J. and Kalafut, P. (2002), *Invisible Advantage: How Intangibles Are Driving Business Performance*, May, Perseus Books, Philadelphia, PA.
- McGee, J. and Prusak, L. (1993), *Managing Information Strategically*, John Wiley & Sons, New York, NY.
- Marquardt, M. (1994), *Global Learning Organizations*, Irwin Professional Publishing, Burr Ridge, IL.
- Neef, D. (2003), *Managing Corporate Reputation and Risk*, Butterworth-Heinemann, Burlington, MA.
- Nonaka, I. and Takeuchi, H. (1995), *The Knowledge-Creating Company*, Oxford University Press, New York, NY.
- Taub, S. (2002), "More corporate crimes and misdemeanors", *CFO.com*, September 16, available at: www.cfo.com