2006

Information Policies and Practices of Knowledge Management(KM) as Related to the Development of the Global Aviation Information Network(GAIN)- An Applied Case Study and Taxonomy Development

Jeffrey S. Forrest
Nova Southeastern University, jeff@forresteducation.com

Information Policies and Practices of Knowledge Management (KM) as Related to the Development of the Global Aviation Information Network (GAIN) – An Applied Case Study and Taxonomy Development

by

Jeffrey S. Forrest

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Science

Graduate School of Computer and Information Sciences
Nova Southeastern University

2006

We hereby certify that this dissertation, submitted by Jeffrey S. Forrest, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Steven Zink, Ph.D.	Date
Marlyn Littman, Ph.D.	Date
John Scigliano, Ed.D.	Date

Approved:

Edward Lieblein, Ph.D. Dean, Graduate School of Computer and Information Sciences	Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2006

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Information Policies and Practices of Knowledge Management (KM) as Related to the Development of the Global Aviation Information Network (GAIN) – An Applied Case Study and Taxonomy Development

by
Jeffrey S. Forrest

May 2006

The Global Aviation Information Network (GAIN) was initiated in response to U.S. Government policies seeking to reduce airline accidents. GAIN was to disseminate airline or aviation safety information in environments where public disclosure impedes the diffusion of information. Government legislation such as the U.S. Freedom of Information Act and other information policies create risks of public disclosure to those reporting information. Therefore, the problem investigated in this research was to identify and evaluate potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information.

Interactions between GAIN, information policy, and knowledge management (KM) and their impact on the diffusion of information were explored. A generalized taxonomy and ontology of KM was interpreted and presented. This taxonomy represents grounded theory developed from examination of examples and cases of KM contained in the literature. This taxonomy may be used to address challenges related to information or knowledge diffusion in various settings.

A specialized taxonomy and ontology addressing issues controlling the diffusion of airline safety information was interpreted. This taxonomy presented issues related to diffusion, disclosure, and policy that may be used to help design and implement airline safety information sharing systems.

Content analysis and text-mining processes were used to help interpret and develop the taxonomies, ontologies, and recommendations made in this study. This dissertation

presents models for using these techniques to develop taxonomy and related ontology from published documentation and recorded interviews. Practitioners may use the methodology of this study to build taxonomy and ontology in other areas of study.

Inductive reasoning was used to develop potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information within GAIN's community and network of practice. GAIN should evolve into a community of practice serving as an information intermediary to various alliances seeking to share aviation safety information. GAIN should focus on assisting alliances with creating environments of trust, collaboration, and the development of policies and fair processes for addressing public disclosure as a barrier to the diffusion of aviation safety information.

Acknowledgements

I would like to thank Dr. Marlyn Littman, Dr. John Scigliano, and Dr. Steven Zink for their guidance while I accomplished this dissertation. My sincerest appreciation is extended to Dr. Zink for sharing his interests and insights related to knowledge diffusion and information policy. Dr Zink's edification provided the foundation from which this study was developed and implemented.

Special acknowledgement goes to Herr Siegfried Niedek. Siegfried spent countless hours sharing with me his extensive knowledge of global aviation safety information networks. Appreciation is extended to Dr. James Simmons of the Metropolitan State College of Denver for his advice during preparation of this dissertation. I also thank the employees of Megaputer Intelligence Inc. for allowing me access to their software products and consultants.

I wish to thank my wife, Dr. Betsy Forrest, for her support during my doctoral studies. Betsy's love and patience were certainly fundamental to my success at NOVA Southeastern University.

Table of Contents

Appendixes

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Global Aviation Information Network (GAIN)

In 1996, the U.S. Federal Aviation Administration (FAA) initiated the Global Aviation Information Network (GAIN) (Orlady & Orlady, 1999). The FAA developed the GAIN concept in response to U.S. Government policies seeking ways to reduce airline accidents worldwide (Hinson, 1995). The primary mission for GAIN is to identify, collect, analyze, and share airline safety data, information, or knowledge among participating members.[1] GAIN's objective is to diffuse safety information and knowledge that, once analyzed and used, will potentially mitigate or reduce the risk of future airline accidents (Gormley, 1999). GAIN currently exists as an industry-led coalition of stakeholders of the global airline industry (GAIN, 2006a).

GAIN requires the cooperative sharing of information and knowledge across cultural, political, and technological boundaries. Therefore, GAIN's success depends on its ability to interconnect and sustain participation by many cultures, organizations, and individuals. Stakeholders participating within GAIN have been defined as "all facets of the aviation community … airlines, manufacturers, pilots, mechanics, flight attendants,

---

[1] GAIN and many other cases described in this study use the terms "aviation safety information" and "airline safety information" interchangeably. However, GAIN's mission is to enhance the diffusion of airline safety information between domestic and international commercial airlines.

dispatchers, regulatory authorities, the military, academia, suppliers, the insurance industry, and others" (U.S. F.A.A. Office of System Safety, 2002). Protecting the confidentiality or anonymity of individuals and entities reporting airline safety information is essential to developing trust among GAIN and its stakeholders. The potential for legal and cultural prosecution resulting from the public disclosure of stakeholders in GAIN is a barrier to the sharing of airline safety information (Simmons & Forrest, 2005). Schreckengast has stated, "Aviation safety data maintainers and information providers need protection from prosecution and litigation for non-criminal aviation events" (1997, p. 17.2). Subsequently, administrators and members of GAIN are currently developing information and technological policies to establish GAIN as a non-punitive information system. GAIN advocates the creation of global information policies and legislation that will de-identify and offer protection to those that contribute and share airline safety related data, information, or knowledge (Tamuz, 1997).

As a proposed information sharing network, GAIN would be structured as a highly complex, dynamic, and evolving system. Nardi and O'Day (1999) have labeled networks with these characteristics as "information ecologies." Information ecologies are environments or settings consisting of "people, practices, values, and technologies" that facilitates or control knowledge diffusion (Nardi & O'Day, p. 49). Davenport and Prusak (2000), Smith and McKeen (2003a), and Sinclair (2006) categorized management processes and policies within information environments that control the knowledge diffusion as "knowledge management." KM focuses on the leveraging or management of knowledge as an asset or "intellectual capital" (Despres & Chauvel, 2000a, p. 6). From GAIN's perspective, airline safety information is valued as an economic and social asset that national and international airlines should share. Based on this premise, GAIN serves as a potentially viable case of applied KM.

Knowledge Management Taxonomy Development and Diffusion of Aviation Safety Information

Despres and Chauvel (2000a), Maier, Hädrich, and Peinl (2006), and Smith (2000) characterize KM as a developing practice consisting of themes or processes used to manage the creation, manifestations, usage, and transfer of knowledge. An ongoing concern of the GAIN initiative is the identification and assessment of KM processes that may reduce or eliminate barriers to the transfer of airline safety information. Therefore, a taxonomy or "thematic analysis" (Despres & Chauvel, 2000b, p. 69) of KM that focuses on issues related to knowledge diffusion was developed and used in this study to analyze GAIN as a case study. This analysis of GAIN produced results that may help to identify and assess processes of KM that enhance the diffusion of airline safety information.

Statement of the Problem Investigated and Goals Achieved

At the time of this study, the GAIN initiative was currently under development by international or non-government agencies and individual country agencies, domestic and international airlines, and other entities ancillary to the global commercial airline industry (U.S. FAA, 2000a). A major challenge to GAIN initiatives will be to develop policies, technologies, and legislation that will reduce potential barriers to the diffusion of airline safety related information or knowledge (GAIN 2006b; Hart, 1996). The following problem statement and supporting sub-problems outline the key research concerns associated with how this research addressed this challenge.

The Problem Statement and Sub-problems Addressed

The problem investigated in this research was that the identification and evaluation of potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information among various organizations has not been studied. Global information systems, such as the one GAIN proposes, are multifaceted and require taxonomies and tools for study that may exceed those normally associated with the analysis of traditional information systems. Swan and Scarbough (2002) and Wijnhoven (2006) have documented the challenges associated with developing generalized taxonomies of KM. Generalized taxonomies may transcend and apply across organizational or community boundaries. Therefore, a sub-problem in this study was to develop a generalized working model or “taxonomy” of KM that may be used to study global aviation or airline safety information sharing systems.[2] The taxonomy will help to identify KM-related issues or methods that may potentially affect the diffusion of data, information, or knowledge within and among organizations or various communities.

Little knowledge exists about the barriers to information and knowledge diffusion associated with global airline safety information systems. Various members of GAIN have described the complexity of determining tools, processes, policies, regulations, networks, and cultural considerations that characterize a global airline safety information

[2] The concepts of “aviation safety information sharing systems” and “airline safety information sharing systems” are used interchangeably in this study.

sharing system (Hart, 2001; Posluns, 2001). For this reason, a specialized taxonomy addressing issues controlling the information and knowledge diffusion of global airline safety information systems was developed. To address this second sub-problem, issues inherent to GAIN and other similar networks that may affect the diffusion of airline safety data, information, or knowledge were identified, qualified, and compared to the generalized taxonomy of KM. In the last sub-problem, potential solutions addressing the barriers to the diffusion of airline safety information identified in the second sub-problem were developed, analyzed, and presented.

Hypotheses Addressed

1. The fundamental hypothesis of this study is that issues related to KM that can directly affect the diffusion of data, information, or knowledge among organizations can be generalized as a taxonomy.
2. A secondary hypothesis is that processes within GAIN that may affect the diffusion of airline or aviation safety information can be identified and described by processes generalized to the KM taxonomy.
3. The concluding hypothesis is that processes generalized to KM can elucidate solutions to improve the diffusion of airline or aviation safety information within GAIN’s network.

Goals Achieved

A dynamism of KM is the continuous development of new methodologies for interpreting taxonomy and ontology used to enhance knowledge diffusion (Rothenburger

& Galarreta, 2006; Wiig, 1997). Therefore, an essential goal in this study was to develop a new taxonomy of KM characteristics or processes central to the concept of knowledge diffusion.

Stakeholders to the global airline industry and members of GAIN have identified the need for ways to improve the diffusion of airline safety information or knowledge (GAIN, 2006a). Therefore, the primary goal in this study was to identify and assess those KM characteristics identified in the aforementioned taxonomy of KM that may serve as potential solutions to the transfer of airline safety information or knowledge across cultural, political, and technological boundaries.

Relevance and Significance

The needs for developing and practicing processes that support the transfer of information or knowledge have been acknowledged for thousands of years (Despres & Chauvel, 2000b). Societies have recognized that processes of knowledge diffusion can serve as business tools leading to management and competitive advantage (Yates, 2000). Within this context, these processes are referred to as knowledge management (Despres & Chauvel, 2000a; Maier, Hädrich, & Peinl, 2006).

Knowledge management is a viable tool for leveraging personal, business, and social assets (Henry & Pinch, 2000; Lamont, 2006). However, debate exists regarding how to best define, characterize, and apply KM. Authors such as Davenport and Prusak (2000), McElroy (2003), and Pinelli, Barclay, Kennedy, and Bishop (1997) have addressed this controversy and suggested various models and taxonomies that serve to characterize the domain and functionalities of KM. Brauner and Becker (2006, p. 74) and

Despres and Chauvel (2000b, p. 56) have called for research that will help delineate a "sociology" for KM as a body of knowledge. They also suggested implementing additional work outlining central themes and theoretical foundations of KM.

The methodology used in this study was built on existing definitions and operational models of KM. A significant feature of this research was to develop a new KM taxonomy focusing on issues related to public disclosure that may specifically affect the diffusion of airline safety information or knowledge. KM ontology was established through inductive reasoning (Holsapple & Joshi, 2002). Gruninger and Lee (2002) have established the need for new KM-related ontologies designed for sharing or reuse by other domains.

Recent trends indicate that KM will be essential to managing "knowledge transfer in strategic alliances" (Rolland & Chauvel, 2000; Sinclair, 2006). Strategic alliances applied to information or knowledge sharing networks, "have the practical benefit of protecting the identity of partners, concretizing a joint project, and prescribing rights and obligations" (Rolland & Chauvel, p. 226). Rolland and Chauvel affirmed that strategic alliances will vary in structure, such as within and among competitors and non-competitors. A fundamental objective for sharing information or knowledge through a strategic alliance is to facilitate the learning and understanding of activities, processes, or other phenomena. Therefore, a key issue to managing strategic alliance-based networks is to reduce or manage potential barriers of knowledge diffusion.

GAIN is proposing to implement an information network serving a global strategic alliance. GAIN participants are comprised of multinational organizations, government agencies, and individuals that function within various socioeconomic and competitive environments. The primary objective for GAIN is to facilitate the sharing of data, information, and knowledge used to improve safety within the airline industry. Therefore, GAIN is a strategic alliance relevant as a case study in KM. In addition to presenting GAIN as a case study, the subsequent conclusions of this research should enhance the ability of GAIN to collect and transfer airline safety information.

Barriers and Issues

A challenge of this research was the selection of appropriate tools and processes used to build a taxonomy for KM and various information sharing alliances. Text-mining software enhances the building and visualization of information topologies (Schröder, 2006; Wise, et al., 1999). These tools offer a variety of automated features that require careful selection for accuracy in textual relationships and retrieval. A strategy for improving the quality of results from text-mining is to combine software automation with manual interpretation (Potter, 2001). Therefore, this research required development of effective strategies for selecting manual and automated text-mining processes.

The GAIN initiative is an applied case of KM directly related to the leveraging of knowledge as a social asset. Many private and public international concerns manage GAIN. Issues such as the value of shared airline safety information, international politics, and potential liability have made negotiations among the GAIN stakeholders sensitive to outside examination (A. Muir, personal communication, July 26, 2001). At the time of this study, GAIN's Administration Manager, Andy Muir, indicated that GAIN participants do not usually grant interviews or participate in surveys external to its own organization.

GAIN's administration publishes extensive documentation on their World Wide Web home page.[3] These publications summarize, and often present in their entirety, the contents of various meetings, discussions of working-groups, and key expert presentations, reports, and white papers. However, some of these documents may not be complete and there almost certainly exists important unpublished documents.

The Limitations

The first limitation is that it was unknown whether stakeholders to the global aviation industry, especially airlines and their employees, would contribute airline safety information to GAIN. Evidence from the literature shows that fear of punitive, legal, or cultural actions serve as significant barriers to the sharing of airline safety information. The risk of public disclosure and related uncertainty of trust are key threats to the success of airline safety information sharing systems. The global nature of GAIN's proposed network and system for the collection and dissemination of information further amplifies these concerns as barriers to reporting information.

The second limitation was that stakeholders would continue to help develop and implement the GAIN concept. Evidence from the literature indicates that GAIN may be evolving as a community of practice, rather than an airline safety information sharing system. It is unknown how stakeholders in GAIN will modify its original mission and

[3] http://www.gainweb.org/

goals – or to what level they will continue to participate in GAIN as a community of practice.

A third limitation was concerned with the feasibility of collecting interview data from key stakeholders in the aviation industry. The same barriers stated in the first limitation influence the willingness of stakeholders to discuss challenges associated with specific airline safety information sharing systems. Furthermore, issues related to national and organizational security since the September 11, 2001 terrorist attack on the U.S. have decreased the willingness of stakeholders in the aviation industry to discuss issues related to safety.

A fourth limitation was that the interpreted taxonomy of KM presented in this study was ephemeral and subjective to individual interpretation. In the text *A Social History of Knowledge*, Burke (2000) warned that efforts to classify information or knowledge change with time and are disputed by different individuals or factions, each concluding different interpretations in different places. The taxonomy of KM in this study was interpreted through qualitative methodology using inductive reasoning. Aspects related to validity and reliability for these interpretations are discussed in Chapter 3.

The Delimitations

The study was limited to investigating relationships between knowledge management, public disclosure, and the ability of airline safety information sharing systems to collect and disseminate information. This researcher acknowledges that many relational, structural, and cognitive factors influence the success of information sharing systems. However, the research was restricted to studying processes of knowledge management and information policies that address the issue of public disclosure as a potential barrier to the sharing of airline safety information.

The researcher examined aviation information systems directly related to the voluntary or mandatory collection of aviation or airline safety information. Databases established for maintaining compulsory government documentation, such as aircraft inspection and airworthiness, pilot, or medical certifications, were not included. The Canadian Aircraft Register Computer System, Canadian Computerized Airworthiness Information System, and U.S. Accident/Incident Data System are examples of information collection and sharing systems not covered in this study.

Many government sponsored and independent aviation or airline safety information sharing systems designed with the primary objective of identifying safety deficiencies and concerns were examined in this study. Of prime concern were those systems that offer voluntary reporting or a combination of voluntary and mandatory reporting by individuals. Detailed investigations of airline safety information sharing systems established as proprietary between individual airlines or industry organizations were excluded. These systems included automated computer-based networks established between organizations for near-real time-sharing (NRT systems) of airline safety information between trusted organizations. An analysis of the archetypal structure and purpose of NRT systems was not included in this study.

Definitions of Terms

Aviation Safety Information

GAIN is a global initiative seeking to disseminate airline safety information (GAIN, 2006b). Aviation or airline safety data and information can be used to measure or describe issues related to philosophies, policies, procedures, or practices that may help to study, sustain, or improve the social wellbeing of all stakeholders to the aviation industry (Orlady & Orlady, 1999). GAIN will collect, analyze, and disseminate airline safety information for the goal of reducing or mitigating airline aircraft accidents.

The U.S. National Transportation Safety Board (NTSB) defines "aircraft accident" as an occurrence associated with the intention of flight resulting in death, serious injury, or substantial damage to the aircraft (U.S. National Transportation Safety Board Part 830, 1988). The NTSB does not distinguish cause or contributing factors as part of the definition of an aircraft accident. The International Civil Aviation Organization (ICAO) clarifies that aircraft operations resulting in death, serious injury, or substantial damage caused by self-inflicted actions or actions inflicted by other persons are not aircraft accidents (International Civil Aviation Organization, 1994). Therefore, airline safety information related to aircraft accidents does not include aspects related to aviation security, such as the detection and prevention of criminal actions or terrorism.

Aircraft accidents may result from many safety considerations such as human error, operating policies, material failures, and natural phenomena such as weather. Security issues such as criminal activities, deliberate sabotage, or terrorism certainly have caused or contributed to aircraft accidents. Wells (2001) contrasts aviation security with aviation safety by stating the following,

> The subjects of security and safety are not fully interchangeable in a technical sense. Safety usually refers to measures taken against the threat of an accident, whereas security refers to protection from threats motivated by hostility or malice. In an economic sense, however, safety and security are identical; they refer to the control of risk. When the Federal Aviation Administration (FAA) mandates pilot training standards or airport security, it is mandating risk reduction for passengers. (pp. 301-302)

At the time of this writing, the collection and diffusion of security information was not an objective of GAIN. Therefore, this researcher defines aviation or airline safety information (or data and knowledge) as mandatory or voluntarily collected information describing philosophies, policies, procedures, practices, and observations related to aviation safety rather than security issues. The terms “aviation safety” and “airline safety” are interchangeable in this study.

Data, Information, Knowledge, and Wisdom

A significant amount of literature exists regarding the concepts and relationships between data, information, and knowledge (Maier, Hädrich, & Peinl, 2006). For at least 2,400 years, the domains of philosophy, science, and theology have addressed and debated the issue of how to define or best characterize knowledge (Snowden, 2000). Commerce has also embraced this challenge. The global economy now recognizes knowledge as an asset leveraged for economic or competitive advantage (Wijnhoven, 2006). In this vein, the motivation by commerce to exemplify knowledge has evolved from philosophical foundations to economic incentive.

The nature of knowledge.

Knowledge is abstract and frequently defined relative to a specific context or evaluation. In addition, knowledge is also held as both "a thing and capability at the same time" (Snowden, 2000, p. 242). This paradox exemplifies the difficulty of embracing knowledge as something that can be easily structured and controlled. Moreover, knowledge may be documented (explicit) or inherent (tacit) to an individual, organization, or society. Explicit knowledge is the form of knowledge that is most easily controlled. However, explicit knowledge may also contain other forms of knowledge, hidden or embedded (implicit), within documented procedures, practices, or policies (Auditore, 2002; Muralidar, 2000). In contrast, tacit knowledge is subjective to the cognitive processes of each individual. In many cases, individuals "may not be conscious of what they know or how significant it is" (Denning, 2000). Therefore, tacit knowledge is not easily characterized, defined, or controlled (Crowley, 2000). These characteristics provide a challenge to organizations that wish to identify, inventory, manage, or leverage knowledge.

Knowledge as related to data, information, and wisdom.

The abstract quality of knowledge intertwines with the concepts of data, information, and wisdom. Charles Meadow stated, "There is no fully satisfactory answer to the question of what information is" (1992, p. 1). According to Meadow (1992, p. 1), the term information should at least refer to something that (a) is constructed of symbols, (b) contains some level of structure, and (c) can be detected and translated by users of the information. Determining a basic definition for information, such as the one offered by Meadow, becomes difficult when comparing the nature of information to data.

Data as related to information.

Meadow defined a single item of data as “a string of elementary symbols” containing the value of an attribute (1992, p. 21). The value of an attribute is subjective and derived by the user of the data. Ambiguity between the characteristics of data and information exists since it is possible to describe an attribute of data in the same way Meadow has defined information. As with information, it is possible to construct attributes contained within a data source with symbols, each structured and translated to derive meaning by the user of the data.

Data has been defined as “undigested observations, unvarnished facts” that once organized, transform into information (Cleveland, 1985, p. 22). The ambiguity of this definition lies in the difference between process, or organization and use. Meadow (1992) suggested that a way to reduce the confusion between data and information is to focus on whether or not the end user has discovered meaning from the information or data used. Meaning used to derive whether attributes are datum or information “is in the mind of the beholder and not recorded in the symbols [of the attribute]” (Meadow, p. 20). This construct suggests that if the end user is able to assign meaning to attributes contained in data, then that data source becomes information. Should the user not establish value from the attributes of the data, then the source subjectively remains data with no informational value.

Within a similar theme, Ray Kurzweil (1999) has also attempted to clarify the difference between data and information. Kurzweil defined information as a "sequence of data that is meaningful in a process, such as the DNA code of an organism, or the bits in a computer program" (1999, p. 30). Although different in approach, Kurzweil seems to agree with Meadow in that data remains data until the user applies meaning – then the data becomes information.

Kurzweil (1999) has suggested additional criteria for distinguishing the difference between data and information. Information, according to Kurzweil, is meaning translated from data that was unpredictable from both the structure and organization of the data. In this definition, Kurzweil has added the construct of order to Meadow's (1992) basic definition of information. Kurzweil implies that if the order of data suggests highly predictable information, then that information remains data in that it was inherently predictable from the original data source. To Kurzweil, only meaning or value that unpredictably resulted from the interpretation of a data source qualifies as information.

Meadow also provided evidence that information is a probable measure of the "occurrence of a symbol" (1992, p. 21). In Meadow's analysis, if information contains attributes predicted with absolute accuracy, then the value of that information remains nothing more than data to the end user. Meadow also assumes that with complete certainty, the state of a system or end user will remain the same. In this argument, a change in state-of-being is evidence that the end user of the data has detected information.

Kurzweil (1999) does not necessarily share the assumption that information can only be information if it fosters change. He stated that meaning placed on data must only have some level of unpredictability. In addition, Kurzweil also typifies information as something requiring order. Informational order is, “information that fits the purpose” (Kurzweil, p. 30). This criterion suggests that information should contain meaning interpreted from data that has some degree of utility. In contrast to Meadow (1992), Kurzweil stipulated information as meaning that offers utility to the end user, and does not necessarily precipitate change by the consumer of that information.

Both Meadow (1992) and Kurzweil (1999) agree that once the user applies understanding and meaning to information, then that information becomes knowledge. However, an individual’s cognitive framework as related to the acknowledgement of understanding and meaning is subject to variations in personality and social setting (Thomas, Kellogg, & Erickson, 2001). Furthermore, all knowledge is ephemeral in regards to its usefulness, accuracy, and value (Krogh, Ichijo, & Nonaka, 2000; McElroy, 2003). For these reasons, the agreement between individuals in terms of how knowledge is valued or held as truth may vary greatly from one individual to another.

Brittle knowledge.

Complementing the rationale of Thomas, Kellogg, and Erickson (2001), Kurzweil added that knowledge is “brittle” (1999, p. 93) in that it is subject to agreement as to the usefulness in value, or order, by those sharing the same attributes of a knowledge base. Meadow also stated that knowledge is defined as “information shared and agreed on by the community” (1992, p. 23). Knowledge has been characterized as “chunks” (Kurzweil, p. 119) of information having a “higher degree of certainty or validity than information” (Meadow, p. 23). However, the validity or truth inherent to any knowledge is subjective to the agreement by society as to the order of that knowledge. Steven Pinker (1997) made an interesting assessment of truth as a prerequisite in establishing knowledge by stating the following,

> Knowledge is just as perplexing. How could I have arrived at the certainty that the square of the hypotenuse is equal to the sum of the squares of the other two sides, everywhere and for all eternity, here in the comfort of my armchair with not a triangle or tape measure in sight? (p. 559)

In effect, Pinker (1997) is questioning his wisdom as established by the understanding of the knowledge he holds. Wisdom is integrated knowledge (Cleveland 1985) that helps to sustain the cognitive process of reasoning. Meadow defined wisdom as the insight required to recognize "relationships among observations [knowledge] that have not previously been recognized as related" (1992, p. 25). Society would probably view Pinker (1997) as having wisdom in that he understands various relationships of knowledge as applied to geometry. However, he is using wisdom to question the evidence regarding geometric principles (knowledge) accepted by society as truth. In contrast to data and information, the abstract relationships between wisdom and truth make the identification, capturing, and further dissemination of knowledge highly subjective (Kidwell, Linde, & Johnson, 2000).

The brittleness of knowledge illustrated earlier also applies to data, information, and wisdom. The order, as defined by Kurzweil (1999), for each of these categories is subjective to the agreement by society as to the evidence used to accept their validity, or meaning. Pinker suggested as a potential solution to the conundrum of these relationships a collapsing of the problem into "one we can solve" (1997, p. 561). This solution would require that debate regarding the relationships between information, data, knowledge, and wisdom be restricted to specific situations or contexts.

Order and structure of data, information, knowledge, and wisdom.

It is important not to let the complexity of definition undermine the purpose and application of data, information, knowledge, and wisdom. The order and structure of these elements create action, utility, or greater understanding. In response to these concerns, Saint-Onge (1996) offered a practical summary linking the relationships of data, information, knowledge, and wisdom by stating the following,

> Data arrive in our lives and on our desks as dispersed elements. It is only when we compile this data into a meaningful pattern that we have information. As information is converted into a valid basis for action, it becomes knowledge. On achieving wisdom, we implicitly know how to generate, access, and integrate knowledge as a guide for action. As individuals and organizations move through the constructs from data to wisdom, their depth of meaning increases and their interpretation shifts from being highly explicit at the data stage to entirely tacit at the point of wisdom. (From Data to Wisdom section, para. 2)

The concepts of data, information, knowledge, and wisdom are salient to the GAIN initiative and the goals of this proposed research. Based on the evidence and rationale presented in this section, the following definitions for data, information, knowledge, and wisdom are provided.

Data.

Data are elementary symbols that are identified, collected, organized, structured, stored, and disseminated. In order to remain as data, no interpretation is made by the user(s) of the symbols or from its related structure.

Information.

Information is transformed from data interpreted by the user or through some form of analysis. In contrast to data, information implies meaning or value relative to some context or sociology. Information may be identified, collected, organized, structured, stored, and disseminated.

Knowledge.

Information that has been processed to affect potential change or gain utility or value, and is shared and agreed to as truth by various users, organizations, or societies becomes knowledge. Explicit knowledge may be identified, collected, organized, structured, stored, and disseminated. The ability to identify, collect, organize, structure, store, and disseminate tacit and implicit knowledge is subjective and highly debatable (Crowley, 2000).

Wisdom.

The ability to recognize usefulness, value, and relationships from and within data, information, and knowledge is defined as wisdom. The potential of wisdom may be present from the identification and selection of data to the establishment of knowledge as a shared truth. In this way, wisdom runs parallel to the continuum of data, information, and knowledge. Wisdom may also be identified, collected, organized, structured, stored, and disseminated (Cleveland, 1985), and is subject to the concerns of brittleness as Kurzweil (1999) previously described.

Knowledge Diffusion and Knowledge Transfer

The meanings and relationships between the terms “knowledge diffusion” and “knowledge transfer” vary within the literature. Efforts to transmit, distribute, and utilize knowledge are characteristics of knowledge management (Maier, Hädrich, & Peinl, 2006; Pinelli, Barclay, Kennedy, & Bishop, 1997). Alvarez (1998) characterized knowledge diffusion as highly complex and dynamic systems that serve to spread information or knowledge within and among various environments, organizations, or societies. Knowledge diffusion is the chaotic flow of knowledge, controlled only by the boundaries of the affected systems or organizations (Wheatley, 1994).

Knowledge diffusion is both a policy and philosophy. In an historical account of early U.S. government information policy, Brown credited knowledge diffusion as essential to “the well being of society” (1989, p. 287). Brown’s work traced the impact of the social and political need for information and knowledge on the development of early U.S. culture, commerce, and government. He credited the cultural demand for the diffusion of knowledge as a social philosophy fundamental to the economic and political success of American culture (Brown, 1989).

In practice, the term “knowledge diffusion” often interchanges with “knowledge transfer.” However, knowledge transfer focuses on creating knowledge and transferring that knowledge to an end user (Voss, 2001). Knowledge transfer frequently represents specific instances, mechanisms, or processes associated with knowledge diffusion. This perspective suggests that knowledge transfer includes the implementation of diverse strategies and tactics used to facilitate the dissemination of knowledge (Alvarez, 1998; Davenport & Prusak, 2000).

Knowledge diffusion as development and usage of knowledge.

Pinelli, Barclay, and Kennedy (1996) delineated knowledge diffusion as the "production, transfer and *use* [italics added] of knowledge." This definition may offer an overlapping association between the concept of knowledge transfer as offered by Voss (2001) to that of Pinelli, Barclay, and Kennedy's view of knowledge diffusion. In this comparison, Pinelli, Barclay, and Kennedy's position placed emphasis on the development and *usage* of knowledge as essential to the concept of diffusion. The usage of knowledge is essential to the interaction within and among knowledge-based environments. Therefore, knowledge diffusion is a conceptual or "holistic" (Pinelli, Barclay, & Kennedy, 1996, p. 229) approach to describing the deliberate or nondeliberate spreading of knowledge (Glaser, Abelson, & Garrison, 1983) within and among various settings. In this theme, knowledge diffusion is more concerned with tracing the flow or path of knowledge and analyzing what factors act as barriers to the creation, transfer, and usage of the disseminated knowledge.

Knowledge management, knowledge diffusion, and transfer.

The evolution of KM may partially explain the ambiguity between the meanings and application of knowledge transfer and knowledge diffusion. The evolutionary roots of KM stem from the foundations of knowledge diffusion and knowledge transfer. Glaser, Abelson, and Garrison (1983) provided evidence that management processes significantly affect diffusion of knowledge. Authors such as Rolland and Chauvel (2000) and Zack (1999) have described KM as the overall framework or management philosophy for addressing and managing the way knowledge flows. This viewpoint suggests that KM facilitates knowledge diffusion. In addition, recent definitions related to KM also imply that characteristics of knowledge transfer are also inherent to knowledge management (see Appendix A). A review of these definitions reveals that KM includes processes that influence knowledge transfer. Example processes related to knowledge transfer include networks, information systems, security, and learning systems. These definitions offer evidence that KM has blended the concepts of knowledge transfer and diffusion – thereby establishing itself as a concept that may affect both the transfer and dissemination of knowledge. This researcher defines knowledge diffusion and knowledge transfer in the following manner.

Knowledge diffusion.

Knowledge diffusion is a holistic approach to studying or managing how knowledge flows when moving among systems, entities, societies, or other knowledge-based environments. As a domain, knowledge diffusion is a “macro” approach to considering how knowledge flows within and across boundaries. The specific precincts between knowledge diffusion and knowledge transfer may not always be evident and may frequently overlap. However, in this research, knowledge diffusion is a policy or philosophy referencing or advocating the total process of knowledge flow. As an example, the term “knowledge diffusion” may represent an entity’s need for and usage of knowledge. This example might include a vision statement of how knowledge diffusion will affect the entity’s operational setting or perhaps its cultural policies toward the diffusion of knowledge.

Knowledge transfer.

Knowledge transfer is a "micro" approach to studying or managing specific strategies or tactics related to knowledge diffusion. The term "knowledge transfer" is in context with the description of a phenomenon's affect on the flow of knowledge or when describing specific tools that can facilitate the flow of knowledge.

Knowledge Management (KM)

KM is a concept that is complex and difficult to define. Starting in the 1990s, various authors began to qualify the meaning of KM and related methodologies. Many of these definitions have explained KM as a domain of processes and tools used to manage or leverage knowledge for competitive or economic benefit (see Appendix A). However, KM is now recognized as both a management theory (Mattison, 1999) and domain for addressing the diffusion and transfer of knowledge within and among "groups, communities, and networks" (Prusak, 2001, p. 1006). Davenport and Prusak (2000), McElroy (2003), and Sinclair (2006) have also established KM as a key function for the production, creation, and utilization of new knowledge within and among communities and networks.

The challenge of determining philosophies, processes, and tools that could potentially increase the understanding and diffusion of knowledge is not new (Denning, 2000; Wiig, 2000a). Literature and other historical artifacts demonstrate the practice for thousands of years of the processes and modes of thought presently associated with KM. Since the ancient Greeks, societies have practiced efforts to extract and diffuse tacit knowledge within and among social infrastructures and communities (Denning, 2000;

Dueck, 2001). In terms of knowledge transfer, Denning related that "interactive knowledge-sharing mechanisms" such as workshops, professional consultation, human migration, reports, and document filing systems have been used throughout recorded history (para. 4).

Knowledge management and globalization.

Considering the extensive history related to the practice and study of diffusion and transfer of knowledge, it is essential to ask why current literature identifies KM as a new domain. Prusak credited the relatively recent establishment of KM to "globalization, ubiquitous computing, and the knowledge-centric view of the firm" (2001, p. 1002). From an economic standpoint, Prusak defined globalization as the unprecedented numbers of those individuals and entities seeking global trade. Prusak suggested that the global demand for products and services coupled with the reduction of time required to communicate using information technology and the decline of centralized economies have led to the era now known as globalization.

Geographic and social perspectives describe various interrelationships between knowledge and globalization. Bell offered the notion that individuals, entities, and societies strive to manage or control knowledge across settings separated by "space, place, and time" (2000, p. 191). Bell's argument for the evolution of globalization rests on the distributed demand for usable knowledge. Usable knowledge is knowledge considered key to improving the quality of life. The usefulness of knowledge may imply value or utility as an asset to the seeker of that knowledge. Therefore, the sustained usefulness of knowledge is subject to management concerns such as the control "of sources, authority, ownership, access, and ‘proper’ use” (Bell, p. 191). Bell’s argument integrates the relationship of management with knowledge that Prusak (2001) considered fundamental to the evolution of globalization and KM.

Prusak’s second factor contributing to the birth of globalization is the recent "unintended consequence of ubiquitous and transparent computing" (2001, p. 1002). Ubiquitous computing has been defined as a “physical world richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives and connected through a continuous network” (Weiser, Gold, & Brown, 1999, p. 693). According to Prusak (2001), ubiquitous computing has enhanced access and availability of explicit knowledge throughout the world. The global infrastructure facilitating ubiquitous computing reduced the effects of time and place as barriers to discovering and accessing explicit knowledge. However, ubiquitous computing has not decreased the difficulty of capturing or diffusing tacit knowledge. Subsequently, the value of explicit knowledge and associated “know how” required to locate explicit knowledge has decreased, while the value and demand for tacit knowledge have increased (Prusak, 2001).

Tacit knowledge is fundamental to cognitive skills such as decision-making, design, innovation, and leadership (Prusak, 2001; Sinclair, 2006). Societies and other entities value these and other knowledge intensive skills as essential to improving the quality of life or enhancing competitive advantage. As a result, individuals, entities, and societies are now striving to manage the acquisition, processing, and diffusion of tacit knowledge. These efforts are fundamental to the establishment and processes of KM (Prusak, 2001; Srikantaiah & Koenig, 2000) and the knowledge-centric firm.

Prusak (2001) suggested that the knowledge-centric view of the firm is the third contributing factor to the establishment of KM. This philosophy emphasizes the management of information and knowledge in ways that facilitate greater organizational intelligence or wisdom. The ability to create and use new knowledge is an essential competency of the knowledge-centric firm or entity (Wheatley, 1999). Prusak stated that increased capabilities of the knowledge-centric firm are built on “knowledge that is mostly tacit, and specific to the firm” (2001, p. 1003).

Knowledge management and business.

In addition to globalization, Wiig (2000a) related that since the early 1980s, the business environment has also played a role in the establishment of KM. According to Wiig, increased emphasis on developing ways to improve competitive ability was, and still is, crucial to the evolution of KM. New business strategies coupled with global commerce lead to an environment of “sophisticated" customers, competitors, and suppliers (Wiig, 2000a, p. 11). The new sophisticated nature of business requires rapid, innovative solutions to highly complex products and service. This challenge requires new ways to interact and communicate with customers and suppliers. Globalized and highly interconnected competitive forces motivate commerce to consider ways to improve effectiveness and efficiency in all business processes. As a result, business leaders began to focus on ways to understand better the management of knowledge.

As a domain for understanding and managing knowledge, KM initially focused on the integration of existing business processes and theories. Information management, quality management, and human resource management form the basis of KM as a practice (Prusak, 2001). According to Karl Wiig, research leaders in KM began to "think in terms of creation, learning, sharing (transferring), and using or leveraging knowledge as a set of social and dynamic processes that need to be managed" (as cited in Sveiby, 2001, p. 5).[4] These concerns began to explore the relationships between the sociology of the firm and managing knowledge. Ways to cultivate the transfer of explicit and tacit knowledge throughout the organization became a fundamental "building block" to KM. The foundations for taxonomies that attempt to describe the philosophies, theories, methods, tools, and processes that now comprise KM have developed from the study of transferring explicit and tacit knowledge.

Knowledge management - taxonomies and topologies.

Establishing taxonomies or topologies of KM help to define the complex nature of KM. Despres and Chauvel (2000b) and Wiig (2000a) offered extensive examples of KM related taxonomies. KM taxonomies have traditionally placed emphasis on the "plethora of concepts, tools, and techniques of knowledge management" that can support the transfer of explicit knowledge (Grant, 2000, p. 53). These elements include management processes that strive to control ownership, access, valuation and the transfer of knowledge. As a management process, early KM models emphasized the integration of information systems and information management. These processes have traditionally focused on the transfer of explicit knowledge. The potential of KM extends to the creation and usage of new knowledge and diffusion of tacit knowledge (Grant).

Grant (2000) and Srikantaiah and Koenig (2000) recommended the development of new KM taxonomies that address ways to create new knowledge and cultivate the

---

[4] Personal correspondence between Karl Wigg and Karl Sveiby as cited in Sveiby (2001, p. 5).

usage of that knowledge. Grant (2000) further recommended that knowledge generating efforts should focus on reducing the cost of learning and subsequent risks associated with decision-making. These concerns rely on the identification, coding, processing, and diffusion of "embedded" or tacit knowledge (Spender, 2000, p. 159). KM embraces these challenges by seeking ways to capture implicit and tacit knowledge, assign meaning to that knowledge, and apply that new knowledge to problem solving or other innovative activities.

Knowledge management – boundaries, communities, and networks.

Spender (2000) highlighted several concerns KM must address when seeking innovation or new solutions. He suggested that individuals, systems, entities, and societies utilize tacit and implicit knowledge. Around each of these elements, there is a degree of "boundedness" that affects the creation and flow of knowledge (Spender, pp. 161-162). Spende provided examples of boundaries that include psychological processes, access to systems, and cultural values. All of these examples affect the diffusion of knowledge among individuals, systems, cultures, and societies. Therefore, identifying and managing boundaries surrounding implicit or tacit knowledge is a primary function of KM.

In addition to embedded knowledge and boundedness, Spender also highlighted the concept of "public goods aspects" (2000, pp. 163-165). According to Spender, a public good shared across boundaries does not extinguish the supply of that good. Public goods are difficult to value, yet retain value by the user(s) in that they offer utility. As an asset, knowledge is a prime example of a public good. As a public good, knowledge exchanged among entities or cultures should improve some aspect of social concern -- such as safety or security.

Entities or cultures sharing tacit knowledge as a public good are "communities of practice" (Addleson, 2000, p. 153; Sinclair, 2006, p. 178; Wenger, 2000, p. 207). Knowledge-based communities of practice are social infrastructures used to facilitate the sharing and learning of new information or knowledge. Members that seek to share communal resources in order to create greater understanding within a practice or enterprise form these communities (Wenger, 2000). Communities of practice attempt to solve common problems by diffusing or transferring knowledge across boundaries. These boundaries may exist within the organization or among organizations and other societies.

Communities of practice are often examined as case-based examples of applied KM. Nonaka and Reinmoeller (2000) and Lesser, Fonyaine, and Slusher (2000) provided extensive case examples of communities of practice that seek to define, adopt, and apply various taxonomies of KM. In many cases, these examples demonstrate that communities of practice normally reside within information or knowledge-based environments. Each environment is usually comprised of multiple communities of practice that are interconnected and bound together by common interests, educational backgrounds, and shared social obligations (Snowden, 2000).

The networks that bind communities of practice within various knowledge-based environments are "networks of practice" (Brown & Duguid, 2000, p. 141). Brown and Duguid qualified networks of practice as "networks that link people to others whom they may never get to know but who work on similar practices" (p. 141). Networks of practice provide the connections that various communities of practice use to transfer information.

Networks of practice and related information technology allow very little opportunity for direct human interaction. Therefore, communication across networks of practice is primarily explicit, with limited capability for the production of new knowledge.

Brown and Duguid (2000) and Schröder (2006) established ties between KM and communities of practice and networks of practice. Between and within each of these topologies are boundaries affecting the flow of information and knowledge. KM recognizes these topologies and manages the flow of knowledge across their boundaries. The need to manage uncertainty and improve quality of life stimulates demand for the transfer and diffusion of knowledge across various topologies. KM is one potential way to embrace this challenge.

A definition of knowledge management universally applied to all settings has yet to be developed. For the purpose of this research, KM is a domain of study and application addressing the transfer and diffusion of knowledge within and among communities of practice and networks of practice. KM includes philosophies, policies, processes, and tools used to manage boundaries that may influence the transfer and diffusion of knowledge. A key function of KM is the creation of new knowledge and the application of that knowledge as a public good. In this study, KM is a means to managing knowledge in ways that may help to mitigate or reduce the risks associated with global commercial airline operations.

Chapter 2

Review of the Literature

Introduction

The literature presents GAIN as a community and network of practice established for the sharing of airline safety information. Discussions from the literature include relationships between GAIN and industry communities and networks concerned with the safety of global airline operations and barriers to sharing airline safety information.

This literature review begins by investigating the characteristics and settings that help define communities of practice and networks of practice within knowledge-based environments. Discussions explore relationships between these concerns and KM. Evidence from the literature provided examples of barriers known to affect the transfer and diffusion of knowledge within and among communities and networks of practice. A brief history of the evolution of KM leading to the advent of the knowledge worker is included. The literature described GAIN as a U.S. government assisted organization comprised of knowledge workers. Writings also establish GAIN as an organization directly related to KM.

Of prime concern in this research is the issue of public disclosure as a barrier to the transfer and diffusion of airline safety information. Therefore, the review includes a detailed case-based description of the development of GAIN initiatives and policies related to barriers in sharing airline safety information. These descriptions include discussions related to the impact of public disclosure and various national government information policies and legislation on the GAIN initiative. Reviewed material includes other cases related to government-sponsored organizations dedicated to the sharing of aviation or airline safety data, information, and knowledge. In contrast to GAIN, the review presents cases of safety and security information sharing systems for domains such as the medical industry, national security, and business.

Various national government agencies have sponsored many of the aviation information sharing systems described in this review. Government information policies and related legislation create concern and influence the risk of public disclosure to those reporting to aviation safety sharing systems. Therefore, this writing places special emphasis on government information policies such as the U.S. Freedom of Information Act (FOIA) and other national initiatives affecting access to information. These policies and other forms of related legislation may serve as barriers to the diffusion of aviation safety information.

This researcher suggests that KM may influence the effectiveness of knowledge diffusion. Examination of the literature reveals known barriers to the phenomena of knowledge diffusion. Barriers that may impede the implementation of KM are included. The review concludes with a recommendation based on evidence from the literature to examine GAIN as a case study demonstrating the interaction between information policy and KM, and their impact on the diffusion of aviation safety information.

Communities of Practice and Knowledge Management

Published definitions describing communities of practice are extensive. However, the variability of context and application inherent to communities of practice are not as wide-ranging as compared to KM (see Appendix A). The following definitions highlight themes commonly used to characterize communities of practice:

1. "Communities of practice consist of people who are informally as well as contextually bound by a shared interest in learning and applying a common practice" (Snyder, 1997, Abstract).
2. Communities of practice are "tight-knit groups formed ... through practice, by people working together on the same or similar tasks" (Brown & Duguid, 2000, p. 141).
3. "When appropriately supported by the formal organization these 'communities of practice' … are the major building blocks in creating, sharing, and applying organizational knowledge" (Lesser & Prusak, 2000, p. 124).

Communities of practice exist within all organizations and cultures (Lesser & Prusak, 2000; Sinclair, 2006). Lesser and Prusak further described communities of practice as being comprised of "structural, relational, and cognitive dimensions" (p. 123) used to build social capital. Knowledge developed in communities of practice is social capital and transferred or disseminated as a public good. KM methodology is a means to create, share, and apply knowledge as a public good within and among communities of practice (McElroy, 2003; Spender, 2000). Therefore, the integration and application of KM influences the development and evolution of structural, relational, and cognitive elements within communities of practice.

Structural, Relational, and Cognitive Dimensions of Communities of Practice

Structural dimensions used within communities of practice include social and technological networks. Cultural mores such as policies, laws, ethics, and trust contribute to the development of social structures. The "information culture" (Davenport, 1997, p. 84), or attitudes and behaviors of communities toward information or knowledge, can vary depending on social structure. Management of social networks can influence members of a community to make connections, evaluate knowledge, and discover new sources of information (Lesser & Prusak, 2000). Krogh, Ichijo, and Nonaka illustrated how Unilever, a consumer-products company, manages its social network through a program called the "Culinary Knowledge Initiative" (2000, p. 61). This initiative requires regularly scheduled debriefing and sharing sessions that foster the exchange of knowledge. In this example, managing the social network increased the appreciation for learning and the sharing of knowledge.

In addition to social processes, the way a network is technologically structured and secured may also affect the ability to create, access, share, and use knowledge. The cost of technology, data standards, related protocols, and usability are examples of technological factors that influence the effectiveness of networks within communities of practice. Managing these factors in a way that supports increased interconnectivity within a community of practice will facilitate greater sharing of information and knowledge (Davenport, 1997).

A function of KM is to manage social and technological networks within organizations and communities (Davenport & Prusak, 2000; Malhotra, 2000). Careful selection and application of these processes should lead to greater levels of knowledge sharing. The U.S. Federal Highway Administration (FHWA) (1997) has identified the successful implementation of KM as a strategy for managing and disseminating highway safety information among various communities of practice and the public. Knowledge managers working for the FHWA chose knowledge sharing tools such as email subscriptions, discussion forums, and online database retrieval systems that enabled network sharing of highway safety information. The FHWA characterized its effort as an example of a networked community of practice designed to implement and support social and technological networks of practice.

The structural dimensions of social and technological networks are avenues to help facilitate the transfer and diffusion of knowledge. However, culture and related value systems play a crucial role in how social and technological structures evolve within communities of practice (Spender, 2000). Fundamental to the establishment of cultural norms is the flow of personal communication through these structures. Personal communication conducted with colleagues or other stakeholders to a community has been determined to be the preferred way to seek new information or knowledge (Pinelli, Barclay, Kennedy, & Bishop, 1997). This preference evolved from recognition that personal communication is a way to qualify sources of information and reduce information overload. Pinelli, Barclay, Kennedy, and Bishop provided evidence that aviation and aerospace professionals prefer personal communication to other sources, such as libraries and the Internet. Their work illustrated that personal communication improves socialization and is an effective and efficient method for transferring tacit knowledge. Personal communications also establishes trust between the seeker of information and the sources being accessed (Lesser & Prusak, 2000). Therefore, personal communication is a timesaving method used to access and filter knowledge valued and trusted by members within communities of practice.

Individuals conduct personal communications as a way to learn about the cultural norms within a community. For this reason, Lesser and Prusak (2000) described the concern for managing the relational dimension within communities of practice. Through personal communication, community members determine whom to trust, ethical values, and sources of knowledge. Activities such as industry conventions and work group seminars offer opportunities for personal communication. As applied to KM, these types of activities are “knowledge sharing events” (Skyrme, 2000, p. 78). Knowledge sharing events are an integral part of KM strategy and used to transfer tacit knowledge or expertise effectively.

Knowledge management as a tool for managing dimensions within communities of practice.

Davenport and Prusak (2000) and Sinclair (2006) highlighted the importance of KM as a tool for managing the relational dimension within communities of practice. They observed that in addition to formalized social and technological networks, effective knowledge transfer can take place by advocating face-to-face meetings. Furthermore, face-to-face meetings create gatherings where there is "room for choice and time for conversation" (Davenport & Prusak, p. 94). In further support of KM as a framework to implement relational communications, Barclay and Pinelli stated, “Oral communication helps individuals identify and articulate a problem or a task in a solution seeking context, contributes to making tacit knowledge explicit, and may be the single most important factor in sharing ‘metaknowledge’” (1997, p. 925). Therefore, KM methods that reduce the barriers to relational communication will most likely improve the transfer and dissemination of knowledge within communities of practice.

Relational concerns along with the cognitive dimension affect the transfer and diffusion of knowledge within communities of practice (Lesser & Prusak, 2000). The development of social and technological networks along with the way individuals think and apply understanding influences personal communication. McElroy (2003) and Wiig (2000a) maintained that effective KM must address cognitive issues such as how people think, learn, and make decisions while performing intellectual work within communities of practice.

Essential to the cognitive dimension of knowledge diffusion is the issue of learning within communities of practice. The objective for GAIN's proposed knowledge sharing network will be to discover and develop ways to mitigate potential risks associated with airline operations. This objective will require the integration and application of KM processes that effectively match how individuals learn, make decisions, and disseminate knowledge (Wiig, 2000a). GAIN's community of practice will develop knowledge sharing infrastructure used for the discovery, development, and learning of best practices that can be transferred to interested parties within the global airline industry. Successful communities of practice support efforts related to learning, developing practices, and transferring knowledge related to these activities (Brown & Duguid, 2000). KM is essential to communities of practice that seek to use knowledge for discovery and the development of best practices (Barclay & Pinelli, 1997). Communities of practice established within the aviation and transportation industry serve as a means to discover, learn, and share best practices. Barclay and Pinelli described how the U.S. Department of Defense (DOD) and NASA established the *NASA/DOD Aerospace Knowledge Diffusion Research Project* as a community of practice designed to address technological problems associated with flight. This community of practice consisted of stakeholders from academia, government, and industry. The project consisted of organizationally and geographically distributed members who communicated through formal and informal communication networks (Barclay & Pinelli). Structural, relational, and cognitive dimensions of the NASA/DOD community of practice enhanced research, learning, and the diffusion of new technology within and among various communities of practice.

The structural, relational, and cognitive dimensions proposed by Lesser and Prusak (2000) offer a taxonomy for investigating the transfer and diffusion of tacit and explicit knowledge within and among communities of practice. There is a strong association of KM as a practice applied to managing the dissemination of knowledge within each of these dimensions. Additionally, KM may be utilized as a way to design, implement, and manage the networking and knowledge-based infrastructure within communities of practice. McElroy advocated KM as strategy for increasing the capacity of communities and networks to “learn, innovate, and adapt to change” (2003, p. 69). These efforts can lead to improvement and the sharing of best practices.

Communities of Practice and Networks of Practice

Communities of practice incorporate KM efforts that advocate personal communication through face-to-face meetings. However, the Internet and other networking technologies have made possible the evolution of "networks of practice" (Brown & Duguid, 2000, p. 141). Networks of practice consist of members who may never meet face-to-face or learn of each other's identity. Members within networks of practice share information and knowledge through network infrastructure such as databases, online discussion forums, and Web sites.

Networks of practice are complementary to communities of practice (Maier, Hädrich, & Peinl, 2006; Skyrme, 2000). As with communities of practice, networks of practice serve as technological and social structures designed to transfer and disseminate information and knowledge. However, communication through networks of practice is usually indirect and flows through third party channels such as email, Web pages, and listservs (Brown & Duguid, 2000). This factor restricts the social structure and interaction of personal communication between members. Nonetheless, networks of practice are implemented within and among various organizational and community settings. Brown and Duguid (2000) have described the establishment of networks of practice throughout Silicon Valley, and within various organizations such as Xerox and Apple.

A key advantage related to networks of practice is the ability to disseminate information or knowledge across time and geography to relatively large numbers of individuals. Networks are viable for sharing explicit or implicit information. Therefore, these networks are beneficial to members desiring to learn and share previously established best practices concerning specific problems or challenges (Skyrme, 2000).

Networks of practice also provide a way for communities of practice to solicit information or knowledge from individuals who may not directly participate within the community. Skyrme explained how various companies use network related “collaborative technologies” such as the Internet, intranets, groupware, Lotus Notes, and videoconferencing as tools for connecting to sources of knowledge that are external to the community of practice (p. 3).

In contrast to communities of practice, networks of practice may be less successful in stimulating innovation or new knowledge. This potential is due to the relative lack of trust within networks of practice (Brown & Duguid, 2000). Trust has been established as the "single most important precondition for knowledge exchange" (Snowden, 2000, p. 239). Working relationships within communities of practice support higher levels of personal communication leading to increased levels of trust. In describing trust and its relationship to the diffusion of knowledge within communities of practice located in Silicon Valley, Kenney (2000) wrote,

> These are teams of people that have worked together over a sufficient period of time to have evolved a deep ability to read each other, to communicate in highly condensed ways, and to know exactly when and when not to trust an opinion from one another. Within such entities, knowledge gets [sic] created, and when it does, it flows almost effortlessly. (p. xiv)

Without trust, individuals are less likely to share tacit knowledge across networks and within or between communities of practice (Sinclair, 2006). Snowden (2000) described that in such environments individuals are less likely to share mistakes and experiences regarding the reuse of intellectual capital and the new association of ideas. Related to trust is the fear of losing power, status, or demand by sharing tacit knowledge or intellectual capital (Starbuck, 1997). Individuals or experts that create and disseminate valuable information or knowledge maintain their status, competitive ability, and self-interest by guarding processes for creating and disseminating intellectual capital. Stakeholders to networks or communities of practice will often resist new ideas or knowledge that will potentially threaten the value or importance of their tacit knowledge base or expertise (Starbuck). Trust and the proprietary nature of intellectual knowledge are of concern to the practice of KM. KM methods attempt to create networks of practice that can sustain the transfer of information and knowledge. Developing ways to disseminate tacit information within networks of practice is a key challenge. In order to meet this goal, KM must strive to find ways to increase the socialization and collaborative aspects within and among networks and communities of practice (Sawyer, Eschenfelder, & Heckman, 2000).

GAIN: A Community and Network of Practice Established on Microcommunities and Knowledge Management

GAIN is a community of practice dedicated to the development of methods, policies, and processes that will potentially enhance the global transfer and diffusion of airline safety information. The primary objective of GAIN is to create a network of practice that will enable stakeholders to discover, create, and share information and knowledge related to airline safety (Gormley, 1999). Networks of practice provide a way for communities of practice to solicit information or knowledge from individuals who may not directly participate within the community (Brown & Duguid, 2000).

GAIN's network of practice seeks information and knowledge from any stakeholder within the global airline industry. GAIN’s structure includes multiple workgroups that serve as microcommunities of practice. These microcommunities (Working Groups) develop, implement, and evaluate various KM-related processes used within GAIN’s network of practice.

Historical precedents related to government information policy, the social demand for information and knowledge, and the interrelationships between various communities and networks of practice will influence the development and implementation of GAIN. Prior establishment of various aviation safety information sharing systems implemented by other countries affect the advance of GAIN. Visionaries hope that GAIN will act as a catalyst for unifying these established aviation or airline safety information sharing networks “into a more unified and systematic international network” (U.S. F.A.A. Office of System Safety, 2002, p. 8). The following sections describe the evolution of these concerns, and their relationship to the establishment of GAIN. A review of GAIN’s Working Groups and efforts related to KM is included.

Historical Perspective of U.S. Information Infrastructures and Knowledge Management

U.S. history contains numerous examples of local and national government policies designed to facilitate the collection and sharing of information. The essence of current U.S. social and political processes stemmed from the need for information early in the nation’s history. Chandler and Cortada have written about the historical depth of the U.S. cultural need for knowledge as a "love affair with information, and related technologies" (2000, p. iv). In the 18th century, the common need for information united American colonies. Noted historian Richard Brown (1989) recounted how colonists demanded an informed society in order to combat the British Parliament's commercial elitism. These early demands for information led the U.S. to develop what Brown stated as a "dynamic, innovative information culture" (1989, p. 39). The geopolitical spark that eventually led to U.S. independence was based, in part, on access to information, and as well as the divergent government information policies of the British and various colonial governments.

U.S. Government as an Agent for Knowledge Diffusion – Infrastructure, Subsidies, and Policies

Early U.S. governmental leaders were determined not to re-create a social and political infrastructure of information elitism. The new U.S. government was to act as a nonbiased agent, enabling the free flow of information throughout all the states (Brown, 1989). This fundamental policy has been credited as a keystone of the modern Information Age (Chandler & Cortada, 2000), and the U.S. as an economy based on access to information (Rifkin, 2000).

Since colonial times, the U.S. government has served as steward of the nation's informational environment. Early U.S. government policies emphasized both the diffusion of information and the strengthening of related technological infrastructures to overcome distance and physical location as potential barriers of knowledge diffusion. Post-revolutionary government information policy resulted in, " a polycentric array of state capitols and commercial centers all require[ing] presses, as well as timely access to long-distance news" (Brown, 1989, p. 48). The expansions of national economic growth stemming from connected information sources required government policies to support access to information. Nineteenth and early twentieth century commercial growth required face-to-face meetings (Brown, 1989). Responding to this need, the U.S. government subsidized transportation such as stagecoach routes and the railroads. Transportation used to connect remote U.S. territories of the 19th century sustained informational media, such as newspapers and mail. According to Basler (1953-1955, pp. 5-6), in the mid-1800s, various business and political leaders considered railroad transportation as a "never failing source of communication" (as cited in Ambrose, 2000). This generally accepted U.S. value for the railroad further buttressed government arguments for subsidies for the construction of railroads, which eventually connected the U.S. Pacific and Atlantic coasts.

The government also subsidized newspapers and postage mail. Subsidies reduced postage rates for the delivery of newspapers to subscribers and free delivery of newspapers between editors (Lubar, 1993). Related government infrastructure initiatives included developing a system of railroad cars that would act as "moving locations" for the collection and dissemination of postage or "rail mail." Information policies (Post Office Acts of 1792, 1845, & 1851) "subsidized, time-specific information on business and public affairs" (John, 2000, p. 59). These policies also introduced legislative foundations for the postal system to protect the right to privacy and confidentiality of the mail.

Information infrastructure and commerce.

After the U.S. Civil War, government policies accelerated the cultivation of transportation and communication systems designed to support and encourage a growing commercial republic. Experienced gained during the war demonstrated the effectiveness and efficiency of the telegraph to transmit timely information. Railroad companies recognized the value of the telegraph in communicating the status of multiple steam powered trains operating in isolated areas and on a single track (Lubar, 1993; Yates, 2000). Congress passed the Telegraph Act of 1866 in recognition of the telegraph as a safety tool as well as a means for the rapid exchange of information. This act allowed telegraph companies to construct telegraph infrastructure along every mail and railroad line in the country (John, 2000).

While "direct" subsidy played only a minor role in the expansion of the U.S. telegraph system, politically motivated information policies, made the expansion possible.[5] By 1852, demonstration of the telegraph as a highly effective tool for transmitting business, transportation, military, and public safety or emergency information led to strong private sector support for its widespread construction (Lubar, 1993; Standage, 1998). Sub-oceanic telegraph networks were another matter. Under-sea telegraph required supplemental funding by national governments; both the U.K. and the U.S. governments invested indirectly in subsidizing sub-oceanic telegraphs (Standage).

By 1858, the U.S. and other European nations were able to communicate instantly via the telegraph (Standage, 1998). While information sent via international telegraph varied from business to personal communiqué, the international telegraph routinely

---

[5] In 1860, Congress did approve an overland telegraph subsidy act, which, in 1861, connected Missouri to San Francisco (Ambrose, 2000).

transmitted information related to the safety of transportation systems, such as arrival and departure times, emergency instructions, adverse weather, and other potential hazards (Lubar, 1993, p. 90).

Despite policies generally supporting minimal direct subsidy, the U.S. government motivated railroads to grant right-of-way access to telegraph companies through the U.S. Telegraph Act of 1866. The Act ensured priority to the railroads for telegraph access and communication. Great public debate ensued over this policy, which potentially interfered with the fundamental principle of access and the free-flow of information. This policy created a political environment that supported research and implementation of new communication technologies (Graham, 2000).

Information infrastructure and standards.

During the early 20th century, government subsidies designed to encourage development of new information technologies began to be successful. Wireless communication systems such as the radio offered nearly instant and direct communication with users located in widely distributed geographic regions. Radio offered the advantage of a virtual network to any user desiring to communicate in various regions. Ships, railroads, ground vehicles, and aircraft could all use radio to communicate operational, emergency, and other safety related information. However, the volume and frequency of unregulated radio communication eventually became a barrier to the transmission of safety information (Lubar, 1993).

Produced from a concern to protect certain radio frequencies for emergency transmission, the U.S. government created the Radio Commission in 1927. This commission, along with its successor, the Federal Communications Commission, set assigned frequencies (Lubar, 1993) for communications associated with safety and emergency management situations conducted over telephone, radio, television, and eventually space-based communication systems. With the rapid increase of new information systems, government information policy and regulations addressed the need for legislation that would protect and sustain these new tools for safety communication.

Issuing discrete frequencies to radio usage, government continued various efforts to negotiate standards among various IT infrastructures and information environments. As early as 1850, various national governments began to sign cooperative agreements that would govern the access, tariffs, rules for connection, and information content that could be transmitted across sub-oceanic telegraph networks (Standage, 1998).[6] European national governments by the mid-19th century controlled access to telegraph networks and the content of information that flowed across them. With the exception of government agencies, national regulations prevented individuals or entities to transmit coded or secured messages using telegraph networks. The complexity of bi-lateral treaties that established the protocol for restricting coded messages caused great confusion and misunderstanding between European government agencies (Standage). In 1865, members from 20 European states established the International Telegraph Union (ITU). The ITU's primary mission was to address the regulations and policies regarding transmission of coded messages across telegraph networks. In 1865, the ITU influenced governments to reverse this policy and to allow the transmission of codified information using different

---

[6] In 1950 the Austro-German Telegraph Union was formed. Other countries such as France, Belgium, Switzerland, Spain, and Sardinia entered into agreements for the sharing of information over sub-oceanic telegraph lines (Standage, 1998, p. 69).

standards (Standage). This agreement between the ITU member states permitted individuals and entities to transmit and receive coded telegraph messages.

Privacy and access to information.

Within the U.S., individuals sent and received coded messages via telegraph networks. The U.S. government, through various information laws such as the Post Office Acts of 1792, 1845, and 1851, sustained the citizens' right to privacy by permitting coded messages. With limited exception, the U.S. government consistently issued policies that supported freedom of speech (Brown, 2000).[7] U.S. policy recognized that secure or coded communication systems would greatly enhance the ability of businesses to share knowledge (Standage, 1998) and increase the free-flow of timely information. Standards in communication infrastructure within and among information environments supported the successful diffusion of transportation safety information (Lubar, 1993).

Government arbitration and support for standards required policy decision making that balanced the requirement for access to information with that of using standards to control infrastructure. While new communication technologies of the early 20th century increased access within and among various information environments, the U.S. government was determined not to repeat the domination by business over communication systems, such as during the era of the telegraph. Government information policies and legislation concerning antitrust, pricing, and "cooperative standard setting"

[7] The U.S. government did issue policy restricting the freedom to communicate information related to slavery by the common citizen or politician. In 1837, communication regarding slavery was considered a risk to national security and Congress issued a "Gag rule" prohibiting public diffusion of knowledge regarding the abolition of slavery (Brown, 2000, p. 50).

were introduced to ensure a national information structure that facilitated access, privacy, and the ability to communicate in a timely manner (Shapiro & Varian, 1999, p. 305). Shapiro and Varian described current and historical U.S. government information policy as an effort to stimulate “cooperation,” rather than “collusion” between various information infrastructures and settings (1999, p. 305).

Information policy and innovation.

Coupled with the development of information standards, U.S. government information policy has also promoted strategic alliances between key industries and research facilities. These relationships have led to revolutionary developments such as the vacuum tube, microchip, the Internet, and modern satellite communication systems (Graham, 2000). Technological innovations stimulated by government policies have helped to ensure the principles of access and the free-flow of information within the U.S.

Information policy directed toward the development of technology also changed the U.S. national information environment. Information collected and disseminated before the advent of the computer and the Internet increased productivity and competitive capability of service and product industries.[8] Introduction of the computer allowed industry to manipulate and analyze data and information in an effective and efficient manner. Traditional information management before computing technology was a profession considered ancillary to the production of some other product or service.

[8] A significant departure from this characterization would be the usage of information infrastructures to collect, analyze, and disseminate information as related to military operations. Standage (1998) provided evidence of military personnel using telegraph technologies in a strategic theme similar to the modern “knowledge worker.”

Information management.

Yates (2000) has described the historical evolution of information management as processes centered on the development of systems used to improve the dissemination of information across multiple levels of external and internal organizational structures. As early as the mid-19th century, public outcry for increased safety influenced railroads to create new organizational structures that would collect and disseminate safety related information within and among railroads. Railroads began to reconsider the effectiveness of traditional organizational management structures in terms of ability to diffuse accurate and timely safety information. During the mid-1800s, railroads began to adopt a structure of midlevel managers specifically charged with the function of handling and analysis of safety information (Lubar, 1993). The railroad industry is most responsible for developing "middle management" organized for the function of creating and administering information systems (Lubar; Yates). Midlevel managers began to collect, store, and analyze information in central locations that would be reported on a routine or daily basis to senior managers.

The midlevel manager of the 1800s was the forerunner of the data and information-processing manager of the 1900s. Information and data processing became prevalent with the move toward decentralized organizational structures (Yates, 2000). A key characteristic of the information-processing manager was the usage of data analysis consisting of statistical processing control applied to the efficiency and successful operation of the transportation system (Lubar, 1993). Statistical processing and analysis of data provided baseline attributes used to detect known and potential safety concerns. Analysis and interpretation of data provided new insights and knowledge (Wheeler,

1993) regarding operational considerations in both railroad and airline transportation operations. The ability of computing technology introduced a new industry concerned with the production of new information or knowledge.

Knowledge Management and the Knowledge Worker

The modern computer, Internet, and related network infrastructure can support the free-flow of information that has been collected and analyzed. Integrating the computer with communication systems modified the collection and transfer of information to include the analysis of new information or knowledge as a key business activity. This new business strategy of the U.S. economy established the role of the "Knowledge Worker" (Cortada, 2000, p. 197). The philosophy of the knowledge worker is that data and information are the raw materials used for creating or recognizing knowledge as an asset or commodity.

Knowledge workers employ the traditional information management functions of collecting, analyzing, and disseminating data and information. Information managers and knowledge workers qualify, structure, and categorize data so that the recipient gains meaning or benefit from the message. The knowledge worker transcends the traditional role of information management by adding to data and information the elements of knowledge as a transferable asset or commodity.

Knowledge is an asset derived from and residing within the individual (Davenport & Prusak, 2000). Cognitive scientists have suggested that the human mind contains both incipient and acquired knowledge (Kurzweil, 1999). Elements of knowledge or "working knowledge" (Davenport & Prusak) enable cognitive processes individuals need to function or create work activity. As an asset, knowledge can help to develop insight or wisdom as applied to work complexity or improved decision making. The knowledge worker applies processes of KM that attempt to identify and capture knowledge as a facet of value. Knowledge workers also consider KM as a process for implementing knowledge diffusion and ensuring that the receiving community or network of practice absorbs the knowledge transferred.

The U.S. knowledge worker evolved from a long history of government information policy that eventually helped to transform the U.S. economy to one based on information and knowledge (Chandler & Cortada, 2000; Tapscott, 1996). The knowledge worker's economic survival is sustained by working with various forms of intellectual capital and related infrastructures. Knowledge workers create commerce within various information settings whereby their product or service is the delivery of intellectual capital, produced through the identification, collection, analyses, and dissemination of information. These activities and processes have transformed the traditional role of information management to that of knowledge management.

Knowledge-based organizations and knowledge workers focus efforts on processes for increased learning, the diffusion of knowledge, and development of organizational intelligence or wisdom (Bennet & Bennet, 2003). Bennet and Bennet also described the future for KM as developing "intelligent complex adaptive systems" (ICAS) (Bennet & Bennet, pp. 41-42). ICAS and related organizations gain power through shared knowledge and where they behave as "intelligent, self-selecting, self-adapting system[s], continually integrating and processing incoming data and information to determine its actions" (Bennet & Bennet, p. 46). Regardless of the idealistic suppositions related to ICAS, Bennet and Bennet believe that the future of KM will remain dedicated to the challenge of knowledge diffusion and the enhancement of creativity and wisdom.

GAIN as an Initiative in Knowledge Management

The U.S. government's FAA Office of System Safety initiated the GAIN concept. GAIN is a program dedicated to the diffusion of safety information and knowledge. The aforementioned traditions of government acting as a facilitator through subsidy, standards, protectionism, privacy, innovation, and arbitration between various information environments are also factors prevalent within the GAIN initiative. GAIN is a landmark effort in applied KM in the airline industry. Knowledge workers participating within the GAIN network share and employ existing and new knowledge related to operational safety considerations across corporate lines. A major challenge to the GAIN initiative is to determine how, and to what extent, various national governments can and should contribute to the potential success of GAIN as an international effort in knowledge management.

The Need for GAIN and Other Aviation Safety Information Sharing Systems

The worldwide commercial aviation accident rate has remained relatively constant for the past decade. For 40 years prior to this period, the global aviation industry maintained a positive rate of improved safety. During this time, innovations in aircraft technologies and improved flight crew training programs such as crew resource management led to the global reduction of commercial aircraft accidents. The global aviation industry recognizes that increased understanding of human factors and the psychology of stakeholders to the commercial aviation industry are the next challenges to improving the past decade's stagnant level of safety (O'Leary, 2002).

A key strategy for increasing the understanding of human factors and related issues of psychology within the aviation industry is to study contributing factors that lead to human error. Airlines, government agencies, and other professional organizations are pursuing strategies for developing systems that enable error management processes that reduce the potential of airline accidents. In order to mitigate potential human error, O'Leary stated that "what we need now is information on the day to day operational difficulties, stresses and human failures that flight crew, cabin crew, air traffic controllers, aircraft dispatchers and maintenance personnel experience on every one of their working days" (2002, p. 246). Improving airline safety by mitigation of human error requires the collection, analysis, and use of data and information related to the day-to-day operational difficulties experienced by the global airline industry. Therefore, many airlines, government agencies, and other professional organizations are now advocating the development of global aviation or airline safety data and information sharing systems (Blakey, 2003; O'Leary).

The U.S. National Civil Aviation Review Commission (NCARC) (1997) encouraged the development of voluntary aviation safety information sharing systems. According to NCARC, these systems should collect, analyze, and disseminate airline operational safety information to aviation professionals, related industries, and the U.S. FAA. NCARC also advised that trust is essential to these systems and that keeping information confidential is essential to the system's ability to acquire information. Safety information sharing systems are likely to fail should disclosure lead to punitive action, misrepresentation, revealed trade secrets, or increased exposure to liability (U.S. F.A.A. National Civil Aviation Review Commission, 1997).

Public disclosure laws such as the U.S. Freedom of Information Act serve as the greatest threat to airline safety information sharing systems. The NCARC, International Civil Aviation Organization, GAIN, and various national government agencies have initiated or endorsed policies and legislative actions protecting aviation safety information from public disclosure and use in punitive actions or litigation (Baumgarner, 2002). GAIN and other independent airline safety information sharing systems protected from access by government agencies provide a level of protection against national public disclosure policies (Baumgarner, 2002; U.S. National Civil Aviation Review Commission, 1997).

Airline safety information sharing systems also provide advantages that enhance safety strategies for individual airlines. Globally, many airlines do not have the resources, time, or management support for developing clear safety procedures or policies. GAIN, as a community and network of practice, can help to supplement and sustain formalized airline safety programs. Airline safety information sharing systems such as GAIN can save time, reduce cost, provide standardized safety information, and enable access to analytical tools applied to error management ("Management practices vary," 2002).

ICAO (Pereira, 2002), the U.S. National Civil Aviation Review Commission (1997), and many other stakeholders in the international airline industry (Gormley, 1999) have endorsed GAIN as a key strategy for reducing the potential of airline accidents.

Furthermore, industry and national government agencies recognize GAIN as a community of practice dedicated to resolving issues related to the impact of public disclosure on the diffusion of global airline safety information. Addressing this concern is essential to the success of current and planned airline safety information sharing systems.

The Evolution of GAIN and Related Work Groups

As of this writing, an international consortium of participants manages GAIN (GAIN, 2006a). GAIN representatives include the airline industry, national governments, non-government agencies (NGOs), and academia. Each year since its inception, members and others interested in GAIN initiatives meet to plan and report on developments designed to implement the core concepts. The following sections provide a chronological description of GAIN's annual meetings. This historical description of the development of GAIN demonstrates the evolution of applied knowledge management in a case with strong ties to U.S. and other national government information policies.

The First GAIN Conference and Workshops (1996)

GAIN held its first international workshop in Cambridge, Massachusetts in 1996. The objective of this meeting was to develop the groundwork for an international information network that would facilitate the "collection, analysis, and sharing of aviation safety information" (U.S. F.A.A., 2000a). Over 150 individuals from eight countries attended the meeting. These individuals represented a cross-section of entities comprised of industrial, governmental, educational, and professional associations (see Appendix B).

The primary theme for the meeting was to discuss and propose ways to develop a "proactive" airline safety knowledge and information network. During this conference, participants envisioned GAIN as a strategy for sharing safety information applied to the mitigation of airline accidents. KM is recognized as a strategy for managing aviation or airline safety information and knowledge in a way that would reduce the potential for future accidents (Lebow, Sarsfield, Stanley, Ettedgui, & Henning, 1999). One of the primary utilities of KM as a management concept is that it should be a means to "instill a sense of crises before it exists" (Davenport & Prusak, 2000, p. 64). This workshop established the potential of future aviation accidents as a crisis requiring the determination of ways to diffuse and transfer airline safety information and knowledge.

Christopher A. Hart, Assistant Administrator for System Safety of the FAA, presented an overview of the GAIN concept (Hart, 1996). Hart stated that government, industry, and labor should share the responsibility of developing GAIN as an initiative toward "Zero Accidents." Hart further stated the following,

> By enhancing our ability to identify risks and develop corrective interventions, government safety regulators and the industry would be able to use their respective safety resources proactively and more efficiently, to their mutual benefit. Through access to flight data and incident reports, an ability to link with data from other sources, and application of various innovative information management and analytical capabilities, all segments of the aviation community would benefit -- insurers, manufacturers, carriers and other operators, pilots, mechanics, air traffic controllers, airport operators, and government. (Overview section, para. 1)

Participants to the workshop also established the vision, objectives, and initial operating policies for GAIN (see Table 1). GAIN's mission statement was "Facilitate the exchange of de-identified air safety information based on trust in real time, with industry participants, providing complete protection to information sources in a cost beneficial

Table 1. Vision, Objectives, and Initial Operating Policies for GAIN as Established During the First Workshop

Category	Description
Vision	GAIN will encourage on-going feedback from participants and users, and will be designed to capture knowledge and expertise.
	GAIN will be dependable and usable, and will allow for real-time access to accurate, quality information.
	The benefits of the process [collecting, analyzing, and sharing] will clearly outweigh the costs.
	The process will be industry-owned and self-regulated.
	Information in GAIN will have adequate protection from liability, embarrassment, and exploitation.
	Management and facilitation of GAIN will allow access to reliable information usable for corrective action.
Objectives	Build trust.
	Demonstrate prototype [information sharing network].
	Establish standards, security protocols, and analytical processes.
	Produce timely, accurate results.
	Provide feedback to verify reliable results.
	Include global participation and support.
Policies	Offer user-friendly, interactive, automated tools for operation.
	Feature confidential, accurate, verifiable source information.
	Create an open architecture adaptable to user needs.

Table 1 (continued).

Category	Description
Policies	*What GAIN Must Not Do*:
	Increase legal vulnerability or be politically motivated.
	Exceed costs required to provide information.
	Be used for regulatory enforcement.
	Accept unreliable data or corrupt existing valid data.
	Use information for other than the GAIN mission.
	Withhold data from benefactors.
	Grow too fast or become too complex too early.
	Be bureaucratic or punitive.

Note. As presented in “The Vision of GAIN” (GAIN, 1996b) and “What GAIN Could Do” (GAIN, 1996c).

manner, ultimately eliminating aircraft accidents (GAIN, 1996a). Key challenges identified by the workshop included developing trust within GAIN’s community and network of practice, effective and efficient diffusion of airline safety information, and the potential of regulatory enforcement resulting from the sharing of airline safety information.

The first workshop also identified potential obstacles and solutions to the implementation of GAIN (see Appendix C). Primary concern focused on determining ways to improve participation within GAIN by stakeholders to the global airline industry (GAIN, 1996a). Cultural change by all potential stakeholders was determined as a fundamental requirement necessary for increased participation within GAIN. Culture was also an issue related to other obstacles such as GAIN's structure and leadership, security issues, information and communication standards, financing, and acquisition and analysis of data and information (GAIN, 1996a).

The meeting included a series of presentations featuring existing models of knowledge sharing. These presentations highlighted examples that showed "how critical information collection and analysis issues have been addressed in [existing] proactive safety systems" (U.S. F.A.A., 2000a). Other proactive systems presented included health care, information infrastructure security, and various transportation systems. These systems served as models to the convention participants for consideration in development of the GAIN system. The Committee on Quality of Health Care in America was highlighted as a particularly poignant initiative to mitigate errors within the health care industry through the sharing of information and knowledge related to medical practices (U.S. F.A.A., 2000c).

The first GAIN conference also saw the formulation of five GAIN Working Groups. These groups were to address the following issues in future meetings: (a) Information Sharing Proof-of-Concept, (b) BASIS as a Working Model Prototype, (c) Aviation Safety Data Sources, (d) Data De-Identification, and (e) a GAIN Web site. Subsequent sections of this review discuss the findings, recommendations, and conclusions by these working groups.

The Second GAIN Conference and Workshops (1997)

GAIN held its second workshop in London in 1997. The objective for this meeting was to continue the momentum of the GAIN initiative started at the 1996 conference. Specifically, this meeting addressed (a) identifying the types of information needed for proactive accident mitigation, (b) identifying obstacles and potential solutions to implementing the GAIN information and network system, and (c) expanding and empowering the number and diversity of stakeholders contributing to the GAIN initiative (U.S. FAA, 2000b). As with the first meeting held in 1996, the conference hosted speakers who presented topics ranging from international concerns to legal issues. The primary event of the meeting consisted of status reports made by each Working Group established since the first GAIN conference. Appendix D provides a categorical breakdown of attendees to the conference.

Working Group I - information sharing proof of concept.

The Working Group on Information Sharing Proof of Concept explored information sharing strategies that might serve as a framework from which to structure the GAIN concept. Working Group I functioned as a microcosm of the GAIN concept and consisted of a panel of six industry members. The group reported, “We believed that we could develop some data provided by the members [of Working Group I] which we could agree to share in order to show the synergistic effect of shared knowledge” (Dalton, Glenn, Wojciech, Parker, Romanowski, & Chang, 1997, p. 15.1).

The group chose several aviation related issues that were determined to be relevant to the sharing of operational safety information. Topics proposed included (a) non-stable approach, (b) asymmetric thrust, (c) thrust reverser variance, and (d) engine vibration (Dalton, et al., 1997). Each group member participated and shared information relevant to each of the selected operational safety issues. Specific airline records or government and manufacturing databases were available for reference. Group members and their affiliated organization could also voluntarily contribute both tacit and explicit knowledge related to the safety topics.

Working Group I identified several significant barriers to sharing operational safety knowledge. The group reported to the conference that it was “hampered from the start by having a lack of active participation by a U.S. airline” (Dalton, et al., 1997, p. 15.1). The group’s consensus was that U.S. airline carriers viewed the risks (e.g., regulatory, enforcement, competition) associated with the disclosure of airline safety information as overshadowing any benefits to participation (Dalton, et al.). The group also discovered resistance by members’ organizations to agree contractually to share “even a limited amount of data” (Dalton, et al., p. 15.1).

Group I identified a third barrier to information sharing as the difficulty in defining data versus information. The group defined information as data analyzed by “knowledgeable interpreters” (Dalton, et al., 1997, p. 15.1). The group expressed concern that raw data related to airline operational considerations and shared over a network could be open to misinterpretation. Misinterpretation could occur by those seeking to derive meaning from the data but lacking the knowledge base or analytical capability to interpret the data. The group viewed this issue as a potential detriment to safety since unqualified entities or individuals could reach false conclusions. As a result, the group concluded that only airline safety information, rather than raw data be disseminated over the GAIN network (Dalton, et al.). Working Group I further recommended that industry experts identify sources and collect data about airline safety related information to be contributed to the GAIN network. These experts would then analyze and interpret the data. The conclusions derived from these analyses applied to solving operational safety issues (Dalton, et al.). The group determined that a major barrier to this strategy would be framing the contractual agreement among GAIN stakeholders to share data on a continuous basis. Traditional information sharing among airlines has been on a case-by-case basis, offering limited potential for the ability to interpret thoroughly all sources of data related to a specific operational safety issue. The lack of an established information network has severely restricted the ability of third party industry stakeholders to access or contribute data or existing information that might be critical to enhancing flight safety. In contrast, Working Group I expressed the hope that GAIN's open network structure would encourage the sharing of information among many industry experts. The group stated, "There is always a benefit to sharing information between knowledgeable people because of the synergistic effect it has on the thought process" (Dalton, et al., p. 15.2).

In their conclusions, the group provided documentation outlining the synergy of evaluating information in selected areas of airline operations. For example, in the case of engine vibration, the group's information sharing developed a synergy that provided a statistical baseline for operational performance monitoring and preventive maintenance (Dalton, et al., 1997). The Working Group I presented this and other examples of synergy through shared information as problem-solving and investigation methodologies applied to airline operational safety information.

Without significant elaboration, the list of potential barriers to knowledge diffusion included (a) legal, (b) cultural, (c) managing large amounts of data, (d) lack of a central network related organization, (e) network infrastructure cost, and (f) the large number of airline operational safety issues the group identified (Dalton, et al., 1997, p.

15.3). The group emphasized that government policies should provide regulatory and legal relief to airlines that participated in a network such as GAIN. However, the group did not offer specific recommendations regarding such policies. Despite the considerable obstacles, the group challenged airlines to, “rise to the challenge” of participation through representation and sharing of airline operational safety information (Dalton, et al., p. 15.3).

Working Group II - the BASIS prototype.

Working Group I identified, investigated, and evaluated potential models for the sharing of information related to selected airline operational safety issues. In contrast, Working Group II performed an analysis of the existing British Airways (BA) Safety Information System (BASIS). BA developed BASIS in 1990 as an information management tool that would help reduce risk by fostering “an open reporting culture” (Holtom, 1997, p. 16.1). Since its inception, the BASIS program has collected safety data that is incorporated into risk management matrices (Schreckengast, 1997).

Working Group II reported that BASIS operates as a fully functional, aviation safety information system. The group also described BASIS as an information network that had already demonstrated many of the attributes proposed in the initial GAIN concept. According to Holtom (1997), the group provided the following description of BASIS and its accomplishments,

> There are over 60 BASIS installations worldwide providing access in one form or another for over 160 airlines and helicopter operators. BASIS Safety Information Exchange (SIE) has been operational for two years and supplies data under protective agreement to more than 80 aviation organizations. De-identified data on 18,000 safety incidents occurring in 1996 was recently distributed to

> contributors. All those incidents include risk assessments and keyword categorizations made by safety professionals to a common format. (p. 16.1)

GAIN asked Working Group II to evaluate BASIS as a prototype safety information system. This evaluation attempted to merge three other selected data sources into the existing BASIS system. The group solicited the Air Line Pilots' Association (ALPA), NASA's Aviation Safety Reporting System (ASRS), and British Airways to contribute data related to Flight Management Systems safety issues. All three entities participated by permitting GAIN to use its BASIS Safety Information Exchange (SIE) software application to attempt to access, merge, and correlate their databases. The ALPA and BA information systems successfully merged into BASIS. However, the ASRS database failed to merge with BASIS SIE (Holtom, 1997).

NASA designed ASRS to track U.S. interests in aviation safety trends (Holtom, 1997). In contrast, British Airways designed BASIS SIE for the identification of risk factors associated with the day-to-day operations of an airline. Industry experts had categorized the data contained in the ALPA and BA databases using a database structure specifically designed to accommodate specific airline operations. According to the group, this difference made it difficult to formulate and filter searches keyed into the ASRS database.

Working Group II succeeded in conducting the formulation and retrieval of searching for data contained in the merged BASIS SIE database. They reported the retrieval of 47 flight management system related incidents along with some cursory interpretation (Holtom, 1997). The group also offered a list of recommendations (see

Table 2) that they believed would improve the utility and value of information and knowledge potentially collected and distributed through the GAIN system.

Working Group II identified differences in cultural values as one of the most significant challenges of an open information network. In assessing the issue of using GAIN to reach zero accidents, Holtom stated, “There are too many elements outside our control, such as terrorism, human error, cultural differences, [and] industrial disputes” (1997, p. 16.3). Societies have varying perceptions regarding issues such as value of life, social structure, and trust.

Table 2. Summary of Recommendations by Working Group II for Improving the Utility and Value of Information and Knowledge Disseminated by GAIN

Category	Recommendation
Data bias	Attempts should be made to collect and share data from as many viable sources as possible.
Integration	A universal taxonomy, or coding system, needs to be developed that will support the categorization and structuring of non-aircraft technical factors (e.g., design faults, operational mistakes).
Corporate culture	A corporate culture supporting trust, honesty, and respect - established by each participating entity to ensure accurate and relevant information. Confidentiality for individuals contributing information maintained and protected.
Corporate management	Airline managers must recognize the safety as well as economic advantages for collecting flight operational data.
National government information policies	National governments must standardize their control over the legislative and legal processes that govern national and international airline operations.

Table 2 (continued).

Category	Recommendation
Analytical policies	Data interpreted for both reactive and pro-active concerns. Proactive analyses should be the priority over reactive.
Airline operational standards	Airline operational standards and policies identified and conformed to on a global basis.
Mitigation	Individuals, entities, or elements identified as a risk or hazard are addressed, prioritized, and rectified.

Note. Summarized from "Proceedings of the Second Global Analysis and Information Network (GAIN) Conference" (GAIN, 1997).

Holtom (1997) further believed the absence of a single agency or central network to control the operations and legislation of domestic and international airlines would act as a barrier offering little chance of improving airline operational safety issues. Emphasizing this point, Holtom noted that crucial differences in cultural values posed difficulties for information managers charged with motivating various entities to collect standardized safety data across national boundaries. It also reintroduced the issues of "trust, sensitivity, and politics" as applied to access and confidentiality between different cultures or political bodies (Holtom, p. 16.4).

The integrity of information networks as an agent for exchanging of information depends on all system stakeholders being trustworthy (Davenport & Prusak, 2000; Holtom, 1997). Holtom emphasized that concerns over trust might be improved through agreements and legislation to protect GAIN participants from future changes in government and network policies, as well as changes in stakeholder participants.

Regarding trust and perception, Holtom (1997) suggested that GAIN, BASIS, and future networks keep their data sharing systems independent from the FAA and other government entities. All Working Group II members concurred that the FAA would be required under the U.S. Freedom of Information Act or other U.S. laws to open access to the database.

Consequently, Working Group II recommended maintaining BASIS as an autonomous network independent from governmental control. BASIS, GAIN, or other future information sharing networks would operate like an Intranet, rather than an Internet.

Working Group III - aviation safety data sources.

During the second GAIN conference, Working Group III reported on its attempts to inventory and describe potential barriers to airline safety related data and information diffusion. The group believed that GAIN stakeholders would have to address these barriers in order to ensure a viable information network. Working Group III was to identify GAIN related characteristics that “ensure all aviation safety data are available for immediate use in accident prevention” (Schreckengast, 1997, p. 17.2). Working Group III also provided the conference with a list of potential data and information sources that could serve as databases in the GAIN concept.

Schreckengast’s (1997) report for Working Group III provided a categorical list of potential barriers to sharing information over networks. These categories included (a) network operating costs, (b) data security and integrity, and (c) criminal and civil litigation (Schreckengast, p. 17.2). These barriers were further qualified as issues that the

GAIN administration must address in order to form the basis for a successful information network.

The group's primary concern was the issue of "trust between and among the end users, data providers, and regulatory agencies" (Schreckengast, 1997, p. 17.2). The group recognized that trust must be the underpinning of any system of information sharing designed to uncover contributing factors to safety related incidents.

Schreckengast (1997) listed specific barriers to information diffusion essential to GAIN. The first of these issues Schreckengast labeled as "media bias" (p. 17.2). In this case, media bias is the extensive broad-based publicity various news and entertainment groups devote to aviation-related incidents. Working Group III identified media bias as a contributing factor to the reluctance by stakeholders to contribute data to the GAIN effort.

In addition to the issue of media bias, GAIN must de-identify and keep confidential contributed safety sensitive information (Schreckengast, 1997). Without de-identification and security, contributors to GAIN would be fearful of media exposure to their particular safety concerns. Exposure and publication of sensitive information could have significant economic, competitive, and legal ramifications to the contributor. Examples of these consequences include (a) the termination of employment for reporting data or information deemed negative by the employer, (b) contributing information or knowledge that may divulge operational processes critical to competitive strategies, and (c) legal action taken against the contributor for reporting data or information revealing the violation of regulations or laws. The group also viewed the potential for litigation as a strong potential barrier to data sharing. Schreckengast stated, "Aviation safety data maintainers and information providers need protection from prosecution and litigation for non-criminal aviation events" (1997, p. 17.2). He also provided evidence that without this protection, entities within the airline operational environment would not be able to foster a "corporate climate" that will sustain data sharing (Reason, 1997).

Related to issues of litigation resulting from identified disclosure, Working Group III also highlighted how differing national Civil Aviation Authorities' (CAAs) policies created potential barriers to data sharing (Schreckengast, 1997). Schreckengast proposed national CAAs ensure collected safety information be used only for issues in safety. CAA information policies should "store and insulate the data provider with de-identification and protection in order to ensure continued voluntary data submission" (Schreckengast, p. 17.3).

In addition to the barriers associated with publicity, government policies, and litigation, the group also expressed concern over the cost and integration of equipment related to supporting the GAIN concept. Specifically, the group identified the cost of aircraft equipment that would be required to monitor safety information (Schreckengast, 1997). Schreckengast reported that issues of human factors associated with the operation of equipment during actual flight would also pose a challenge to the GAIN concept. Complementing the issue of onboard information equipment was the challenge of standardizing the software and processes used to analyze and present safety information (Schreckengast). This concern was for both safety information processed and displayed during flight as well as post-flight information provided as feedback for expert interpretation.

Working Group III presented socio-economic concerns as another significant potential barrier to the sharing of data and information within the GAIN network. The group noted that the accident rates for underdeveloped or developing countries were typically several times greater than that of the U.S., United Kingdom, or Europe (Schreckengast, 1997). Countries with higher than average accident rates were anticipated to be the least likely to participate in GAIN financially.

Table 3 provides a summary of Working Group III's recommendations made at the second GAIN conference. Working Group III made no specific recommendations regarding how to implement and manage the recommendations made.

Table 3. Concerns and Recommendations Made by Working Group III Regarding Barriers to Knowledge Diffusion

Concern	Recommendation
National legislation	Introduce legislation to protect individuals from punishment or litigation for voluntarily reporting incidents and non-standard occurrences.
Management and resources	National aviation authorities should supply the management and infrastructure required to collect, analyze, safeguard, and disseminate aviation safety data and information.
	Government and industry must supply, install, and financially support the necessary hardware and software requirements of GAIN to ensure economic compatibility and international standards.
Education and research	Implement industry-wide training related to safety data collection and procedures.
	Undertake research to complement or enhance GAIN's efforts to define and mitigate human performance deficiencies.

Table 3 (continued).

Concern	Recommendation
Processes	Provide industry recommendations to local organizations in order to enhance International Civil Aviation Organization reporting and analysis procedures.
	Industry must use current data and provide unbiased analyses using best business practices and government standards.
Diffusion of knowledge	Government and industry must recommend safety changes for inclusion into airline training programs.
	Industry will record and report data or analyzed anomalies to respective administrators. Administrators will remedy or warn users of the deficiencies.
	Governments will disseminate knowledge derived from GAIN to other transportation systems.

Note. Summarized from "Proceedings of the Second Global Analysis and Information Network (GAIN) Conference" (GAIN, 1997).

Working Group IV - de-identification.

Without proper methods for de-identification, GAIN data and information might expose data contributors to varying degrees of risk. Essential to the success of GAIN is the need to protect the identity of sources contributing data or information. Working Group IV's task was to evaluate the issue of de-identification.

Working Group IV defined de-identification as, "The removal of identifying information from data to protect the confidentiality of data providers" (Tamuz, 1997). The group's primary objective was to consider governing policies and database architectures that would balance the need for a viable network while protecting the data providers' identity. Such protection is essential to the concept's success. Exposure of identity could subject the source to competitive damage, legal actions, and forms of punishment specific to the various cultures involved in the disclosure.

As was Working Group III, Working Group IV expressed concern over potential misuse of data. Misuse could occur when contributed data is used in a manner contrary to the source's intention. An incident of data misuse risks breaking the trust between the source of the data and stakeholders to the database. The working group noted that such access and misuse would result in the reluctance of individuals, entities, and nations to contribute to the database. Tamuz characterized the potential for the misuse of data as a form of "unintended access" to the GAIN database (1997, p. 8.5).

The GAIN database should filter identifying information in order to protect sources from the potential misuse of their data. However, de-identification is not without costs. The value of shared data in analysis and interpretation is more compelling when the data retains the context originally contributed. Data filtered for de-identification can inhibit the ability of the analyst to discover new meaning, or subtle nuances to patterns (Tamuz, 1997). Discovered patterns or relationships found within the GAIN database may lead to new knowledge furthering the safety of airline operations. The policy issues for de-identification would need to balance the building of trust through protection while sustaining data quality that can support viable analysis and interpretation. The management of these policies can potentially affect the diffusion of existing data and the dissemination of new information. Policies allowing access to the identification of all sources might deter the flow of information since contributors are more likely to fear the misuse of data and related consequences. Alternatively, policies of strict de-identification may also decrease information diffusion since data providers may question the utility and value of interpretations made from the data contained in the database.

Various Working Groups recommended database management and network structuring as a means to guard against the misuse of data and information contained within the GAIN system. One way to provide such protection was through a segmented database and retrieval system separating autonomous control and access by individual entity or state.

Working Group IV - proposed GAIN segmented database.

In order to seek a balance between de-identification and analytical utility, Working Group IV proposed a “segmented database” (Tamuz, 1997, p. 8.9). The GAIN database would be comprised of three separate computer storage facilities located within the national boundaries of three countries. One country would host a database containing the field keys linking sources to data elements. A second database located in another country would contain the actual source data identifying the contributors to the GAIN system. A third database would contain those elements considered “benign” to the source (Tamuz, p. 8.10). This database would be open to all members of GAIN - subject to approval processes managed by a governing board of elected GAIN officials.

Selected GAIN employees would use an additional computer for inputting small batches of contributed data and information sources. The input computer would be used only to segment and transmit the data to the three independent and nationally located databases and not to archive GAIN related information permanently (Tamuz, 1997). Tamuz maintained that the small batch processing conducted on this input computer would reduce the chances of a GAIN employee detecting patterns or meaning while inputting the data.

Countries hosting the GAIN databases would be selected based on "favorable legal climates" (Tamuz, 1997, p. 8.9). Such a distributed system would require lawyers to contend with multiple legal systems in any attempt to request information. It would also impede the ability of those attempting access to GAIN on the grounds of national legislation. Of prime concern was the potential for ease of access through the U.S. FOIA.

GAIN elected advisory and confidentiality boards would manage the entire database (Tamuz, 1997). These boards would manage researchers' requests to obtain access to the complete GAIN database through coordinating with all contributors of the requested data. In any event, the contributor to GAIN would retain the right to insist on keeping sensitive data confidential.

In addition to the GAIN Advisory and Confidentiality Boards, GAIN staff members would also serve as intermediaries or "honest broker[s]" between those requesting data and the sources of the data (Tamuz, 1997, p. 8.16). According to Tamuz, GAIN intermediaries would confirm the identity and requests for sources of data, release identifying fields on approval of the GAIN advisory boards, and assist in the formulation and delivery of special requests or data interpretations. The intermediaries would also ensure that encryption is used for all data or information transmitted within the GAIN infrastructure.

Tamuz (1997) characterized the GAIN segmented database, advisory boards, and staff intermediaries as information structures offering protection against the misuse of data. In terms of information and knowledge management, the policies and infrastructure of GAIN's proposed segmented database were to (a) impede attempts to subpoena data, (b) act as a barrier to the U.S. FOIA, and (c) protect against internal and external unauthorized access.

Working Group V – GAIN Web site.

The second GAIN meeting recognized the need for an official GAIN Web site. It was determined that the Internet and related Web-based technologies would support the vision of GAIN (Booker, 1997). Booker described that the GAIN Web site would publish administrative information regarding GAIN and related activities. Access to proprietary information would not be made available through the site. For security reasons, access to shared safety information should be made available through intranets rather than the Internet (Booker, 1997). In response to concerns regarding the security of sharing safety information over the Internet, Booker stated that, "You will have to learn to work through trust to get over your fear of safety data on the Internet" (Working Group #5 section). Booker added that communication and awareness builds trust, and these factors must exist before a network shares data or information (Booker). However, participants to the conference feared that either proprietary or non-proprietary safety information made available on the GAIN Web site would be misused (Holtom, 1997). Therefore, participants suggested evaluating proprietary intranets as the primary infrastructure for sharing proprietary airline safety information.

The Second GAIN Workshop also sought the perspectives and concerns of various stakeholders regarding the implementation of GAIN. These groups included representatives from airlines, pilots, European aviation agencies, lawyers, and aircraft manufacturers. Concerns that were common to the First GAIN Workshop, such as confidentiality, indemnification, and participation remained prominent. Murphy (1997) suggested that consultants seemed to have dominated the initial interest in GAIN. Commercial vendors or consultants that would potentially supply GAIN with technologies and related processes would likely recognize economic incentives for their participation within GAIN. Table 4 summarizes other concerns stated during the Second Workshop.

Table 4. Summary of Perspectives and Concerns Regarding Barriers to the Implementation of GAIN Expressed During the Second Workshop

Category	Concerns and perspectives
Legal or statutory	Various European and U.K. courts subpoenaed protected safety information from existing aviation safety information systems.
	Intellectual property, indemnification, commercial usage, and common law indigenous to various cultures require consideration.
Integration	GAIN should not compete with or disrupt the viability of existing aviation safety information sharing systems.
	Establish standards for data analysis. Develop improved tools for data mining and visualization.
Stakeholder participation	Stakeholders may question the quality of data, information, or knowledge shared within the GAIN system.
	Stakeholders may not see the need or benefit to participate.
	Management demands required for participation may exceed the ability of various airlines to participate.
	Certain cultures or organizations may be in conflict with each other, and will not participate in the same network.

Table 4 (continued).

Category	Concerns and perspectives
Stakeholder participation	Pilots are resistant to participating within information sharing systems. They fear issues related to confidentiality, disciplinary, administrative, civil, and criminal liability. Anonymity is required. Participation is more promising for networks within an organization rather than between organizations.
Policy and processes	How should data be de-identified, and within what period should data be available for access before de-identification? Under what circumstances will the U.S. FOIA be invoked to permit access by the public to data and information held within GAIN. Data and information overload.
Diffusion of knowledge	How will GAIN distribute new knowledge? Focus should be on the transfer of "lessons learned."

Note. Summarized from "Proceedings of the Second Global Analysis and Information Network (GAIN) Conference" (GAIN, 1997).

The Third GAIN Conference and Workshops (1998)

The Third World GAIN Conference, held in November 1998, focused on issues and solutions to barriers of sharing airline safety information and the development of related analytical tools. Presentations included case studies demonstrating advantages for collecting and analyzing airline safety information. Hart (1998) opened the conference by challenging GAIN stakeholders to find solutions to the legal barriers that may impede the sharing of confidential airline safety information. He stated that the development and standardization of tools used to analyze airline safety data and information must be a priority of GAIN.

The proposed structure for GAIN and related policy issues began to shift during this conference. Hart (1998), Bozin (1998), and Logan (1998) suggested that rather than a segmented or centralized database, GAIN should be comprised of a network of databases maintained by the organization or entity owning the source. Logan and other conference representatives described how organizations that collect and disseminate safety information within their own organization recognize economic advantages through risk reduction. Data and information networks within the airline industry tend to be more successful when dedicated to a single organization (Logan, 1998). Logan added that organizations that own, maintain, and control small, highly focused databases tend to produce higher quality data, leading to improved efficiencies within the organization. Hart (1998) suggested that GAIN would remain a privately owned and voluntary system regardless of the evolving network structure.

Conference members described processes for identifying and collecting airline safety data and information. These examples defined data as facts, unedited reports, and quantitative details (Griffith, 1998). Griffith described information as a synopsis of analytical and descriptive details derived from data and corrective actions. Methods used by various airlines for collecting safety data and information included (a) crew air safety reports, (b) digital flight data analysis, (c) proprietary confidential reporting systems, (d) employee interviews and meetings, (e) meetings with the FAA and manufacturers, and (f) training programs (Clark, 1998; Doguet, 1998; Mancini, 1998).

Flight Operations Quality Assurance (FOQA).

The goal of zero accidents also shifted during this conference to the reduction of fatal accidents by 80% (Matthews, 1998). This change reflected a policy shift by the White House to reduce fatal accidents associated with U.S. airline operations by the year 2007 (U.S. Department of Transportation, 1998). Matthews noted that one of the primary strategies for this reduction is the implementation of Flight Operations Quality Assurance (FOQA) and related Digital Flight Data Recorder systems (DFDR). The DFDR unit is an onboard monitoring computer that records aircraft systems and performance along with crew control, airmanship, and behavior. FOQA is comprised of various analytical techniques, tools, and processes used to interpret data generated from DFDR databases (Simmons & Forrest, 2005).

Compared to other national airlines, FOQA has been less successful in the U.S. European airlines and many other national carriers have successfully implemented FOQA initiatives (Matthews, 1998; Orlady & Orlady, 1998). European airlines have traditionally treated the data and interpretations derived from FOQA as confidential and non-punitive. Matthews suggested that the U.S. supports a "punitive culture" (Punitive Culture section) in regards to error, while other nations view inadvertent error as part of human nature (see Table 5).

Within the U.S., people fear reporting mistakes since the outcome for sharing information about errors is punishment (see Table 6). According to Matthews, the punitive culture within the U.S. acts as a significant barrier to the transfer and diffusion of confidential data and tacit knowledge. Orlady and Orlady (1999) described cases within the U.S. of individuals and legal agencies attempting to use FOQA to identify

Table 5. Variations of Cultural Values Regarding the Treatment of Human Error Discovered Through FOQA by the U.S. and Other Nations

FOQA - U.S. cultural values	FOQA – values by other nationals
Find out who was responsible.	Inadvertent errors are not punished.
Blame those responsible.	Inadvertent mistakes are treated as symptoms of a problem.
Prevent future problems by punishing or seeking compensation from those responsible.	Symptoms are used to identify adverse trends and avert problems before they become serious.

Note. As presented in "Freedom and an Open Society – Road Blocks to Improving Aviation Safety in the U.S.A." (Matthews, 1998).

and blame flight crews for various performance violations. The potential of disclosing FOQA information in court proceedings or for the prosecution of regulatory violations has created a significant barrier to the implementation of FOQA within the U.S.

In contrast to the arguments made by Matthews (1998), Orlady and Orlady (1999) provided evidence that punitive cultural values affect aviation or airline safety information sharing systems throughout the world. Crewmembers in New Zealand, Indonesia, France, and Japan are punished from violations of various regulations and procedures discovered through FOQA. Orlady and Orlady (1999) described the fear and consequence of punitive culture as related to incident reporting by stating the following,

> Unfortunately, fear of litigation, fear of regulation, and fear of punitive action still impedes and sometimes prevents meaningful incident reporting in most parts of the world. The belief that punishment is indispensable and society's best protection against transgressions of any sort is an intrinsic part of many national, regulatory, and corporate cultures. (pp. 397-398)

Table 6. Fears and Concerns of Airline Personnel, Governments, and Regulators Indigenous to a Punitive Culture

Personnel	Fear or concern
Line personnel	"Loss of Face" by peers.
	Punitive action by management, regulators, or civil authorities.
Management	Punitive regulatory action.
	Legal action and discovery.
Government agencies or regulators	Media bias, legal action, and public perceptions.

Note. As presented in "Freedom and an Open Society – Road Blocks to Improving Aviation Safety in the U.S.A." (Matthews, 1998).

In addition to cultural values as applied to human error, FOIA is an additional significant barrier to the transfer and diffusion of airline safety information within the U.S. (Griffith, 1998; Matthews, 1998). Matthews characterized stakeholders in the U.S. airline industry as less likely to contribute confidential knowledge to government regulators since FOIA requires the release of that information or knowledge upon request of the public. While Matthews acknowledged that FOIA supports democracy and legal processes, he attributes FOIA as a major barrier to improving airline safety through the sharing of data, information, and knowledge. FOIA was a central theme at the Third GAIN Conference and subsequent GAIN meetings.

FOIA and disclosure issues during the Third GAIN Conference.

During the Third GAIN Conference, Matthews (1998) suggested that FOIA should not apply to confidential information collected for improving public safety. This modification would apply only to data or information describing inadvertent errors or mistakes. Griffith (1998) stated that "Exemption 4" of FOIA be modified to include initiatives such as GAIN and FOQA. Exemption 4 "protects 'trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential'" (U.S. Department of Justice, 2002, para. 1). In response, Matthews (1998) agreed that modifying FOIA would be highly beneficial to GAIN. However, he warned that passing modifications to FOIA through the U.S. Congress would be the most difficult challenge facing the GAIN initiative (Matthews).

Jaeger (1998, Overview) also addressed FOIA by suggesting that policies and legal acts protecting the right of "privilege" for information disclosed during legal action be adopted by FOIA. Jaeger cited examples of legal protections that if recognized throughout all U.S. jurisdictions, could ensure confidentiality of information collected by GAIN from FOIA disclosure. These protections, referred to in some cases as "Safety Privileges" (Jaeger, 1998, Legal Protection) or "Self-Critical Analysis" (Kolczynski, 1998, Discovery), are recognized in various military and U.S. civil actions when information is collected under the promise of confidentiality and applied to public safety. Under these protections, those seeking to protect the confidentiality of information must prove that disclosure will harm the future ability to collect information that may sustain or improve public safety.

In addition to legal protections, the Third GAIN Conference also examined policies of the International Civil Aviation Organization that might protect the disclosure of confidential aviation safety information. The ICAO's structure of approximately 185 contracting states establish policies regarding practices and standards as applied to air commerce. In regards to issuing international policy related to aviation information sharing systems, the ICAO (2001) later adopted Resolution A33-16: ICAO Global Aviation Safety Plan (GASP). GASP advocates the following,

> 10. *Urges* all Contracting States to examine and, if necessary, adjust their laws, regulations, and policies to achieve the proper balance among the various elements of accident prevention efforts (e.g., regulation, enforcement, training, and incentives to encourage voluntary reporting) and to encourage increased voluntary reporting of events that could affect aviation safety, and instructs ICAO to develop appropriate policies and guidance in this respect… (International Civil Aviation Organization, 2001, operative clause 10)

As with GAIN, ICAO is concerned with finding ways to reduce the impediments to sharing aviation safety information globally (Orlady & Orlady, 1998). ICAO's Annex 13, Accident and Incident Investigation and Prevention, specifically addresses concerns related to the collection and dissemination of airline safety data resulting from an aircraft accident or incident. Paragraph 5.12 of Annex 13 established that the justice in each state would not disclose confidential information related to an aircraft accident or incident unless "disclosure outweighs the adverse domestic and international impact such action may have on that or any future investigations" (McCarthy, 1998, p. 5.12). McCarthy described legal cases where parties applied Annex 13 as a legal defense for the protection of confidential data and information. A New Zealand court argued the use of Annex 13 had a limited binding force and posed potential conflict to police and related investigations (McCarthy, 1998). According to McCarthy, the court noted that provisions such as Annex 13 regulate the use of information rather than restrict its usage. Under this opinion, courts determine on a case-by-case basis the admissibility of data or information protected under Annex 13.

McCarthy (1998) related that policies (such as Annex 13) regulating rather than prohibiting the use of airline data and information have created resistance by airline crewmembers to various data and information gathering tools. Tools such as the cockpit voice recorder (CVR) record verbal communication of the flight crew (Simmons & Forrest, 2005). FOQA uses CVR systems and data to collect and analyze airline safety data or information. Crewmembers fear that the CVR and other flight recorder monitoring devices could be used against them in "subsequent disciplinary, civil, administrative, and criminal proceedings" (McCarthy, 1998, Attachment D section). Therefore, McCarthy warned that airline crewmembers would most likely resist sharing such information with voluntary data and information sharing systems.

The Third GAIN Conference suggested that the U.S. National Transportation Safety Board (NTSB) store and manage data and information collected by GAIN. The NTSB is responsible for collecting, maintaining, and analyzing data and information pertaining to civil aircraft accidents. With certain exceptions (see Appendix H), data and information held by the NTSB is accessible by the public or through FOIA. However, the NTSB would not be partial or very effective in disseminating the data and information collected by GAIN (1998). The opinion also stated that the NTSB would classify all data and information collected from GAIN as privileged and confidential. According to the opinion, protections such as classifications "work only on information not seen by a lot of people, and we need safety information to be widely distributed" (GAIN, 1998, Conference Summary). This debate concluded with an additional opinion supporting GAIN as a privately owned and maintained entity.

Perspectives of GAIN and information sharing and disclosure made during the Third GAIN Conference.

Benoist (1998) provided the Third GAIN Conference with an overview of challenges to data sharing from an aircraft manufacture's perspective. According to Benoist, Airbus (a large European aircraft manufacturer) has considerable experience in the development and implementation of data sharing systems. The Airbus data sharing systems collect and share data, information, and "lessons learned" from sources internal to the business, as well as a network of client operators. Benoist deemed the following characteristics essential to support successful airline safety information sharing systems:

1. Pilots report all significant anomalies and mistakes.
2. Events are analyzed using collected flight data.
3. Analyses of data and information are disseminated and statistics are developed.
4. Information dissemination is quick and reliable.
5. Databases contain consolidated data and appropriate taxonomy.
6. Design, procedures, and training are frequently updated and shared along with lessons learned.

Key elements to data information sharing systems must include high levels of participation, trust, confidentiality, and legal protection to participants. Benoist (1998) emphasized that information sharing systems that hold data as confidential rather than anonymous are more effective in collecting quality data and offer better potential for analysis. Confidential data and information sharing systems enable owners of the database to conduct follow-up actions with collected and analyzed data. Benoist also stated that analysis and dissemination of lessons learned are the value-added benefits to airline safety information sharing systems.

Garaufis (1998) described the FAA's position regarding GAIN and information disclosure. He stated that the FAA "cannot ignore the interests of several affected parties when considering the protection of safety information, including the media, tort lawyers, and victim's families" (Garaufis, 1998, Conference Summary). The FAA supports initiatives that share and protect aviation or airline safety data or information. Garaufis (Conference Summary) added that while the FAA "can waive, in advance, any punitive enforcement action based on information collected under FOQA, [it is also] required to retain the capability for remedial enforcement." Furthermore, U.S. law establishes the responsibilities of the FAA. Therefore, the FAA would not participate in efforts to change existing laws regarding the disclosure of confidential aviation or airline safety information.

The FAA also acknowledged that GAIN is an initiative directly related to knowledge management. During the conference, Garvey stated, "while businesses are using knowledge management for strategic advantage against their competitors … we in aviation are … using this approach to achieve collective advantage" (1998, para. 4). Garvey added that GAIN is an applied case of knowledge management stimulating the cooperation and sharing of information between national and international civil aviation authorities and the private sector. The FAA's central role in supporting GAIN is to help eliminate barriers to the dissemination of data and information across national boundaries (Garvey). According to Garvey, the FAA is reducing barriers to knowledge diffusion by soliciting the participation within GAIN of international civil aviation authorities, such as ICAO and member states. The FAA is also integrating domestic safety initiatives with GAIN and producing analytical tools to analyze the data and information contained within the GAIN database (Garvey).

The Fourth GAIN Conference and Workshops (2000)

At the Fourth GAIN Conference, Hart (2000) emphasized that public disclosure issues, potential job sanctions, criminal proceedings, and civil litigation against future sources contributing to GAIN remained as barriers to the diffusion of airline safety information. However, data and information collection test cases conducted by working groups within GAIN and the data produced by FOQA resulted in evidence that information overload and the need for related analytical tools would serve as a significant barrier to the GAIN concept. Hart described information overload as a more formidable barrier than legal impediments to sharing information within the GAIN infrastructure. A key agenda for the conference participants was to focus on the development of data analysis tools that would help to overcome the challenge of information overload within GAIN.

Hart (2000) also emphasized recent U.S. government information policies that could potentially help the GAIN initiative. The Federal Aviation Administration Reauthorization Act of 1996 prohibits the public disclosure of voluntarily provided safety or security aviation data collected or shared by the FAA. Under this Act, the FAA

Administrator may refrain from disclosing aviation safety and security information once established that disclosure would deter future voluntary sharing of that type of information. The Administrator may also keep confidential any data or information established as essential to “fulfilling the Administrator's safety and security responsibilities” (Federal Aviation Administration Reauthorization Act of 1996, § 402). However, the Federal Aviation Administration Reauthorization Act of 1996 does not supersede any other provision of U.S. law, such as FOIA. The Federal Aviation Administration Reauthorization Act of 1996 was also issued to the public as notice of proposed rule making (NPRM) that would protect “airlines and their employees from enforcement actions for regulatory violations discovered from voluntary reporting programs” (Hart, 2000, Removing U.S. Obstacles).

The Fourth GAIN Conference announced the adoption by ICAO of policy for the sharing of airline safety information. The Accident Investigation Group ’99 (AIG) of ICAO established that, “States should promote the establishment of safety information sharing networks among all users of the aviation system and should facilitate the free exchange of information on actual and potential safety deficiencies” (McCarthy, 2000, ICAO AIG ’99 section). ICAO also recommended that states develop laws supporting non-punitive voluntary reporting systems that feature standardized database formatting capable of the timely dissemination of information (McCarthy, 2000). Hart (2000) and McCarthy (2000) stated that the safety information sharing policies issued by ICAO would potentially motivate states to incorporate the GAIN initiative and encourage the development of laws that would facilitate participation by stakeholders.

As a strategy for developing laws that would enhance the sharing of aviation safety information, ICAO established that it would “undertake a study of international law with a view to discover provisions pertaining to the protection of confidential data and, if necessary, to propose solutions” (McCarthy, 2000, ICAO AIG ’99, section). In addition to legal considerations, ICAO recommended that entities within the airline industry develop formal sharing agreements. These agreements would facilitate the sharing of “sensitive safety information [that] would be shared only to the extent permitted by its owner and owners could share to a different extent with different entities” (International Civil Aviation Organization, 1999, Discussion).

While in support of the GAIN concept, ICAO recommended that existing and future aviation safety information sharing networks work together to develop formal sharing agreements. ICAO suggested that formal sharing agreements could provide protection from punitive actions while sustaining the nature of voluntary sharing networks. ICAO (International Civil Aviation Organization, 1999, Discussion) identified the following additional characteristics and potential benefits of formal sharing agreements that may enhance the dissemination of aviation safety information:

1. Formal agreements allow for the articulation of processes that may help assure the adequate protection of shared information.
2. Information can be structured such that access is issued to appropriate or “need to know” users.
3. Agreements enable validation and quality control processes and standards that help to ensure understanding and appropriate use of shared information.

4. Contracting partners establish standardized terminologies, definitions, taxonomies, formats, and network protocols.
5. Customize the form and composition of reports to meet the needs of specific parties to the agreement.
6. Information is disseminated at pre-specified periods.
7. Agreements specifying information standards, content, and frequency for distribution may facilitate the analysis and comparison of data and information over time.
8. Agreements may enable participants the opportunity to follow-up with sources in order to ascertain additional information.
9. Airlines have established a preference for establishing sharing agreements between airlines, airframe, and engine manufacturers.

Participants at the Fourth GAIN Conference established the need for international government support for the GAIN initiative. In response, committee members implemented the Government Support Team (GST), which began deliberations in October, 2000 (GAIN, 2002a). Initial types of government support viewed helpful to GAIN are research actions, development of standards, and regulatory actions (Angerand, 2000). Examples of government agencies that could potentially support GAIN were identified as civil aviation authorities, accident investigation boards, and air traffic services (Wojciech, 2000). Wojciech also suggested that these types of agencies could provide technical and administrative resources to GAIN. The following list identifies other specific government support functions and GST activities that could help the GAIN initiative (Angerand, 2000):

1. Develop laws that enforce non-punitive information sharing environments.
2. Increase awareness of existing and planned government aviation safety information sharing systems.
3. Disseminate lessons learned from previous information sharing efforts.
4. Develop prototype information sharing systems for use by GAIN stakeholders.
5. Encourage international data standardization.
6. Research and develop data and information collecting tools for use by GAIN stakeholders.
7. Research and develop data and information analytical tools for use by GAIN stakeholders.
8. Help establish aviation safety information data analysis laboratories that are independent of regulatory agencies.
9. Help motivate airline industry members to participate within GAIN.
10. Provide administrative and consulting support to GAIN.
11. Coordinate GAIN activities among high-level government authorities.

The Fifth GAIN Conference and Workshops (2001)

The Fifth GAIN Conference held in December, 2001, assigned the GST responsibility for promoting the GAIN initiative. GST goals included identifying potential solutions that may reduce barriers to the sharing of airline safety information (Predmore, 2001). GST government and non-government members (see Appendix I) were asked to identify and describe barriers to sharing airline safety information within and among organizations and cultures indigenous to their respective nationalities. The

GST identified four primary impediments to safety information dissemination as (a) civil litigation, (b) regulatory sanctions, (c) criminal proceedings, and (d) public disclosure (Sayce, 2001).

Sayce (2001) observed that none of the GST countries offered protection against civil litigation or regulatory sanctions for the reporting of information that is required by regulation. However, all GST member countries offer some level of protection against public disclosure for information that is voluntarily submitted (Sayce). According to Sayce, protection against criminal proceedings varied greatly among the GST nations.

The SST identified cultural values and reward systems as two factors greatly influencing the characteristics of barriers to airline safety information and knowledge sharing. Tendencies toward prosecution or "criminalization" are predominate in France, Japan, the U.K., and the U.S. (Sayce, 2001, Criminal Proceedings). Sayce noted that Australia, Canada, and New Zealand offered varying degrees of cultural and legal policies that offered protection against regulatory and criminal actions resulting from voluntarily submitted information. New Zealand advocates a cultural policy of "just culture" (Sayce, Criminal Proceedings). A just culture is as an "'open' culture where [flight] crews are encouraged to discuss their mistakes or problems in the expectation there may be lessons to be learned by everyone, but penalties were most unlikely" (Ward, 2001). Ward also described that just cultures should offer rewards to those sharing safety information that leads to improved performance and reduced accident rates by flight crews.

A cultural environment that supports the value of just culture must balance the natural propensity for human error with the need for accountability and justice. As with the GAIN initiative, the medical industry has sought to create a just culture that balances the effects of human error, trust, and blame on the diffusion of information and knowledge (Roberts, 2001). Roberts illustrated the nature of just culture and the responsibilities of a society seeking to improve the quality within the medical industry by providing the following rationale,

> However, when it comes to assessing the level of responsibility, potential for punishment or censure, it is society's responsibility, as a just culture to assure that that natural human characteristic, to blame, is balanced with natural justice, a fair hearing and an appropriate level of reparation to all victims. In the conduct of a professional practitioner, this also requires a high level of understanding the context in which mishap occurs and the differentiation of voluntary or willful damage, performance beyond one's capabilities or inadvertent bad luck. (para. 7)

Roberts (2001) also added that a just culture is a learning environment based on policies that impede blame. According to the GST, government's responsibility to formulate non-punitive policies and legal structures will facilitate the sharing of information within learning environments (de Courville, 2001). de Courville wrote that governments should develop policies that help to protect, support, encourage, and reward sources of airline safety information. In characterizing recommended government policies, de Courville (The Actors in the Industry) recommended, "informal networks of people with a good safety culture, committed to share, learn and act is more efficient than a rigid and heavy official process." Within a just culture, it is both the airline industry's as well as governments' responsibility to share airline safety information.

The GAIN Government Support Team and issues of public disclosure.

The GAIN Government Support Team was directed to help "government and industry reduce legal and organizational barriers that discourage the collection and sharing of safety information" (GST, 2001a, p. i). Specifically, GST responsibilities include helping government mitigate legal impediments to the sharing of airline safety information. The GST identified legal impediments as civil litigation, regulatory sanctions, criminal proceedings, and public disclosure.

Central to the problem addressed in this study is the identification and evaluation of potential solutions to policy issues in public disclosure that prevent the collection and sharing of airline safety information among various organizations. The GST defined public disclosure as, "Concern that the information will be disclosed to the public, in the media or otherwise, and used unfairly, e.g., out of context, to the disadvantage of the provider of the information" (GST, 2001a, p. 2). Public disclosure is an impediment limiting the ability of government and existing collecting systems to obtain useful information related to airline safety.

Within the U.S., the fear of public disclosure has created a voluntary sharing environment whereby individuals are generally (a) unwilling to report safety information, (b) reluctant to provide full disclosure, (c) prone to distort information, and (d) discouraged from open cooperation (GST, 2001a, p. A-10). These factors caused the FAA to issue special rulemakings Part 193 and the FOQA Rule that guard against public disclosure of data or information voluntarily collected (Flight Operational Quality Assurance Program, 2003). Other nations such as New Zealand and France have characterized public disclosure as a barrier with minimum impact on the dissemination of airline safety information. The impact of public disclosure on the global sharing of airline safety information varies with the different types of government acts, laws, special databases, special programs, and protections administrated within each nation (GST, 2001a). The following section examines these factors and their relationships to various past, existing, or planned airline safety information sharing programs.

The Sixth GAIN Conference and Workshops (2003)

Meetings at the Sixth GAIN Conference held in 2003 continued to explore potential solutions to technical, legal, and economic challenges acting as barriers to GAIN and other airline safety information sharing systems. Qualifying GAIN’s mission to meet these challenges, Predmore (2003) described GAIN as an industry association dedicated to:

1. Gathering and disseminating information related to aviation safety management processes.
2. Providing a forum for collaboration by industry stakeholders concerned with aviation safety issues.
3. Sharing information regarding tools, methods, and procedures used to collect, analyze, and disseminate airline safety information.
4. Creating an environment that can enable the collection and sharing of airline safety information.

The conference acknowledged that the threat of public disclosure and related punitive consequences remained prime barriers to the dissemination of airline safety information. Specifically, Freedom of Information legislation remains a key barrier to GAIN and other government sponsored aviation safety information sharing systems (Burin, 2003). Hart (2003) announced the need for collaborative efforts between GAIN and other industries concerned with similar barriers to sharing of safety information. According to Hart, GAIN will share best practices with industries and agencies such as healthcare, national security, nuclear power, chemical, and other transportation modes.

The GAIN strategic plans outlined goals for addressing disclosure and related punitive legal actions as barriers to the dissemination of airline safety information. These goals include promoting and facilitating voluntary, non-punitive airline safety information sharing systems and soliciting government support of GAIN (2002b). Individual tasks associated with these goals included:

1. Increase global awareness of planned and current government airline safety information sharing systems.
2. Advocate the importance of developing voluntary, non-punitive safety information sharing systems to government and industry organizations.
3. Promote GAIN activities to governments through demonstration of industry and government collaborations successful in disseminated best practices and lessons learned.
4. Increase awareness by industry and legislative and legal communities of issues that affect the collection and sharing of airline safety information.
5. Facilitate development and implementation of solutions to legal and organizational barriers to the diffusion of airline safety information.

As of this writing, GAIN had not published a categorical attendee list to the Sixth Conference (see Appendixes B-G). GAIN did report that 195 individuals from 23 countries attended the event. The conference also had the largest attendance by airline representatives of any GAIN conference, with 40 airlines represented (GAIN, 2003a).

European Union's Directive Occurrence Reporting in Civil Aviation.

Conference attendees reviewed the European Union's Directive Occurrence Reporting in Civil Aviation. This directive, adopted in 2002 by the European Parliament and the Council of the European Union, established that Member States should develop mandatory aviation safety information reporting systems. Information collected by these systems would be stored in databases and electronically shared to various "entrusted" government and private entities concerned with regulating safety issues, investigating accidents, or improving aviation safety (European Commission, 2002, p. 7).

The European Union's Directive Occurrence Reporting in Civil Aviation also advised Member States not to prejudice legislation protecting the right to access government information. However, each Member State would ensure that the Union's system would not record the identity and address of each reporter to database. The Union's system protects against punitive actions except in cases of gross negligence (European Commission, 2002).

Near-real time airline safety event sharing systems.

Participants of the Sixth GAIN Conference advocated the adoption of near-real time airline safety event sharing systems ("NRT systems") by stakeholders to the aviation industry. NRT systems are "Computer-based systems that allow airlines [or] their airline organizations to share aviation safety information with other airlines [or] their airline organizations via e-mail systems, web-based systems, or transmittal of electronic storage media" (GAIN, 2003b, p. 2). NRT systems provide voluntary, organization-to-organization sharing of safety information. Participating organizations to NRT systems negotiate access rights and the types of information collected and shared.

The primary objectives for establishing NRT systems between participating organizations include the sharing of specific safety issues or events and best practices (Posluns, 2003). Designated airline safety officers usually determine the information collected and disseminated by NRT system members. Participating airlines maintain ownership and control access to their internal NRT database. Each airline de-identifies its database information and may maintain that information or submit it to an independently owned, merged database. NRT systems are not real-time since there is usually a delay from the date of a safety event to the date of access approval (GAIN Working Group C, 2003).

Posluns highlights NRT systems as capable of disseminating secured, de-identified, safety information between participating airlines. Examples of these systems include the International Aviation Transportation Association's (IATA) Safety Trend Evaluation, Analysis & Data Exchange System (STEADES), and AvSoft's AvShare. STEADES is a global NRT system that will serve as an independent airline safety information database and analysis group (IATA, 2003). IATA anticipates that STEADES will eventually serve 95% of the international airline community. Each quarter, airlines release safety information via standardized reports to the STEADES NRT. IATA described STEADES as an open, non-punitive system compatible with other aviation safety information sharing systems.

AvSoft is a privately owned company that produces the AvShare NRT message based system. As an NRT message based system, AvShare serves as a tool for airline safety officers to establish “trusted groups” via the Internet (AvSoft, 2003, para. 2). AvShare encrypts anonymously reported and shared data and information.

The Seventh GAIN Conference and Workshops (2004)

In 2004, the Seventh GAIN Conference was held in Montreal, Canada. Information and proceedings presented at this conference were redundant to many of the concerns presented in previous GAIN conferences. Several topics presented at the conference and related to this study emphasized the application or evaluation of software used to collect flight data or to data mine aviation safety information. No known references to GAIN’s progress as a global aviation information network were presented at the conference, or published in the GAIN Web site.

GAIN in 2006

GAIN did not hold an eighth conference in 2005. In February 2006, Ed Fell of the GAIN Steering Committee announced that the U.S. FAA Office of System Safety had decided to cease funding the GAIN initiative. According to Fell, FAA funding was terminated due to labor shortages and budgetary concerns within the FAA. In an email message sent to GAIN stakeholders, Fell solicited feedback from members to help determine the future of GAIN (E. Fell, personal communication, February 21, 2006).

In his appeal to GAIN’s stakeholders, Fell described the past success of GAIN as, “facilitating the application of methods, tools and processes for the collection, analysis, and sharing of safety-related information within the aviation safety community” (E. Fell, personal communication, February 21, 2006). In his communiqué, Fell did not reference GAIN's past or present intentions to become a global aviation information network.

At the time of this writing, the results of GAIN's efforts to seek a solution to its future are unknown. In April, 2006, the GAIN Web site announced that no future meetings were planned for GAIN's organization. The GAIN Web site also affirmed that it was seeking strategies for continuing as a non-profit entity, supported by dues from organizations and individuals (GAIN, 2006b).

Aviation Information Sharing Systems – Case Examples

The number of private and government sponsored aviation or airline safety information sharing systems is extensive (Simmons & Forrest, 2005). It is not feasible to account for all of these systems (Ranter, 2001) since many are proprietary and are in various stages of development. The following sections profile case examples of national and privately owned aviation safety information sharing systems.

European Government Sponsored Aviation Information Sharing Systems

From a U.S. government perspective, GAIN addresses the sharing of airline safety information on a global basis. While ambitious, GAIN is not the first effort to construct such an information system (Simmons & Forrest, 2005). Since the early 1960s, the European Community has and continues to support several concepts similar to GAIN (Orlady & Orlady, 1999). These examples of applied knowledge management preceded the GAIN initiative in 1995. Henrotte has described these efforts as "Euro-GAIN" information systems designed to collect, analyze, and exchange airline related safety data and information (1997, p. 10.1).

In 1991, the European Commission comprised of 15 European States and 12 partner States announced its intention to disseminate accident and incident aviation safety data in a document entitled "Communication on Community Initiatives Concerning Civil Aviation Incidents and Accidents" (Henrotte, 1997, p. 10.11).[9] This report outlined a proposal to require mandatory investigation for all aviation related accidents. Each investigation would be required to issue a report outlining recommendations that would improve aviation operations. The initiative also emphasized that each report would protect the identity of all individuals and entities involved. The Community and its partner nations would receive all accident safety reports for further dissemination.

By 1994, the European Community had issued additional directives describing policies to refine further the Euro-GAIN initiative. New policies and directives required that the distribution of mandatory aviation safety reports would contain conclusions and recommendations considered valuable to the enhancement of all aviation flight information (Henrotte, 1997). The U.S. GAIN concept emphasized the collection, analyses, and dissemination of information related strictly to airline operations. In contrast, the Euro-GAIN initiative was concerned with collecting information related to both the commercial airlines and general aviation. This implies that the European strategy would collect safety information derived from all commercial and non-commercial flight activities.

---

[9] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom with the contractual additions of Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slavonia, and Slovenia (Henrotte, 1997, p. 10.1).

Variances in government strategies for attracting participation within both information systems account for differences between the U.S.-GAIN airline model and the Euro-GAIN aviation model. GAIN is an information sharing system that will potentially attract voluntary sources of data and information from entities that stand to recognize economic incentives through participation (Holtom, 1997). As a result, the U.S. government focuses on commercial airline operations. In contrast, the Euro-GAIN concept would require the participation of all aviation stakeholders in the community. The Euro-GAIN strategy holds the more ambitious goal to improve all “air” safety (Henrotte, 1997, p. 10.2).

European Communities’ Confidential Human Factors Reporting Program (CHIRP) and the European Confidential Aviation Safety Reporting Network (EUCARE).

In 1993, the European Communities’ Ministers began to seek information systems models that demonstrated protection of confidentiality (Henrotte, 1997). The Ministers learned that the U.K. had been working since 1982 on a confidential aviation related database known as the Confidential Human Factors Incident Reporting Programme (CHIRP). Initially operated by the Institute of Aviation Medicine of the Research Department of the Royal Air Force (RAF), the U.K. Civil Aviation Authority’s Scientific Department, Medical Department, and the RAF funded CHIRP. CHIRP is now an independent chartable trust under U.K. law and funded by a grant from the U.K. Civil Aviation Authority (S. Niedek, personal communication, August 28, 2003; Sullivan, C., 2001). Modeled partly after the U.S. ASRS, CHIRP maintains complete confidentiality of source information (Confidential Human Factors Reporting Program, 2001).

The Ministers next evaluated a system similar to CHIRP referred to as the European Confidential Aviation Safety Reporting Network (EUCARE).[10] Created in 1992 at the Technische Univeristät in Berlin under the direction of Siegfried Niedek, EUCARE was capable of merging various languages into its database. In 1993, the Community adopted the EUCARE system as a test-bed and found the system successful in the solicitation of voluntarily sourced information related to aviation human factors (Henrotte, 1997). EUCARE created a "truly independent, credible, and competent source" of voluntarily contributed aviation safety information (Willumeit, 2001, para. 2). According to Willumeit, the German Constitution's Freedom of Science article protected public disclosure of information and sources held by EUCARE. The Freedom of Science article prevents disclosure of confidential information held by German universities. Niedek maintained that, "All information gathered [by EUCARE] was therefore secure against any attempt to transfer it to any other place" (S. Niedek, personal communication, September 5, 2002). Furthermore, the EUCARE system did not maintain identifying information within its database (EUCARE, 2000).

In 1999, EUCARE was terminated as a test-bed. According to Willumeit (2001), EUCARE was in an ongoing dispute with industry as to how an independent information collection system should operate. In addition to industry pressures, Niedek (personal communication, September 15, 2002) described other contributing factors to the termination of EUCARE (see Table 7). In Germany, information policies related to the right of citizens to access government information are inconsistent within the German

---

[10] EUCARE was an acronym phonetically constructed to be a play-on the English pronunciation "you-care." Since English is the regulatory language within the global airspace system, it was hoped that this meaning would help the adoption of EUCARE by air carriers (S. Niedek, personal communication, September 15, 2002).

Republic. Niedek related that Germany is the only member of the European Union that does not have a uniform national freedom of information policy.

Three states within the German Republic have formal "Informationsfreiheit," or information policies related to freedom of information (Federal Republic of Germany, 2003). These policies provide citizens with limited rights related to the access of information held by government agencies. The German Republic does have a Federal Data Protection Act, which is both state and national law. The Federal Data Protection Act provides, "the basic right of the individual to decide on the use and communication of his or her personal data" (Germany, 1998). The protection against public access to documentation containing individual identities is an essential responsibility of the German government to protect each citizen's privacy. Challenging the protection of privacy in Germany requires conditions of overriding social or national interest.

The Federal Data Protection Act was of great importance to EUCARE. Protection of individual identities existed as long as EUCARE did not de-identify reports. However, the inconsistent nature of German policies related to FOIA, coupled with debate over airline safety as a social concern, led various entities and government agencies to challenge the right of EUCARE to maintain the confidentiality of its reporters. These pressures eventually led to the termination of EUCARE (S. Niedek, personal communication, August 19, 2003).

Once terminated, EUCARE deleted all information contained in its database (Steinke, 2002). Willumeit (2001) also believed that EUCARE's independence from government and industry demonstrated the most effective form of protecting the confidentiality of sources to information sharing systems.

Table 7. Contributing Factors and Their Impact Leading to the Termination of EUCARE

Factor	Impact
Airline industry pressures	Airlines placed political pressure on the German government for the release of source information contributing to EUCARE.
Pilots	In some cases, pilots demanded the release of source information.
Government	Government financial and political support to EUCARE ceased because of political pressure of industry and pilot organizations.
Cultural	The translation of "reporting" in Germany implies the meaning of "required" or "mandatory." Therefore, pilots resisted EUCARE as a directive or order.
	Various governments threatened their national pilots with job security and punishment for contributing information to any aviation safety information system or network.
Procedures	Sources contributed very sensitive information to EUCARE via inappropriate government channels. Information contributed was disclosed publicly. This resulted in a loss of trust by potential sources to EUCARE.

Note. From an Interview with S. Niedek, Founder of EUCARE, September 15, 2002.

European Coordination Centre for Aviation Incidents Reporting Systems (ECCAIRS).

As a test-bed for the Euro-GAIN initiative, the European Community's Council of Ministers established the European Coordination Centre for Aviation Incidents Reporting Systems (ECCAIRS) (Henrotte, 1997, p. 10.2). ECCAIRS served as a prototype information system designed to collect, analyze, disseminate, and report aviation related safety information. ECCAIRS faced challenges similar to the BASIS test model. ECCAIRS was to examine and test the problems of merging various aviation safety databases from Community members that had incompatible information structures (Henrotte). Henrotte described how the structuring of aviation safety information varied from one Community nation to another. During implementation, ECCAIRS determined that member nations had widely varying requirements and taxonomies of terminology for reporting aviation accidents and incidents. The policies and government regulations relating to ECCAIRS members ranged from no requirement to collect or report aviation safety data to mandated safety information systems. The ECCAIRS test-bed also revealed broad variations in handling and analyzing aviation safety data among Community members.

ECCAIRS established that a common characteristic of existing Community databases was that data and information linked to aviation technical problems outweighed data and information identified as related to areas of aviation operational concern. Henrotte (1997) concluded that the imbalance in types of data and information contained in ECCAIRS was due to the lack of government legislation protecting the confidentiality of sources. Human factors associated with operational safety include issues sensitive to individual action or behavior, and were highly susceptible to retribution from authorities. Legislation protecting the confidentiality of ECCAIRS would offer an incentive to those sources wishing to contribute human factors data and information. Government policies, legislation, and technological factors to ensure the confidentiality of Euro-GAIN initiatives might also help enforce an environment of mandatory reporting for all aviation related accidents and incidents.

In 2002, the objective for ECCAIRS, as an aviation information sharing system, was established as "the prevention of future accidents and incidents and not to attribute blame or liability" (Post, 2002, p. 1). ECCAIRS evolved into a system of data analysis tools and databases based on international standards (ICAO ADREP data format). ECCAIRS de-identifies and maintains confidentiality for any information collected or exchanged. Post described the following ECCAIRS policy regarding legal impediments and public disclosure,

> Member States shall not institute proceedings regarding what has been reported under the mandatory occurrence-reporting scheme except in case of gross negligence. Furthermore, national regulation/law must ensure that employers do not subject people, who duly and accurately report incidents, to any detriment. (p. 2)

France's Confidential Event Reporting System (REC) and BEA Aviation Accident-Incident Database.

In France, the Confidential Event Reporting System (REC) is an example of a non-independent aviation safety information sharing system that has succeeded in protecting the privacy of sources to the database. The official French aviation accident and incident investigation agency known as the Bureau d'Enquêtes et d'Analyses (BEA) administered REC. Data collected in the REC program is voluntarily submitted, and related to general aviation (non-airline) (Bureau d'Enquêtes et d'Analyses, 2002). REC uses the data collected for analyses applied to the mitigation of future general aviation accidents and incidents.

The BEA guarantees confidentiality to those contributing data or information to the REC (Bureau d'Enquêtes et d'Analyses, 2002). Source information to the REC is deleted "before exploiting the data of the event" (Bureau d'Enquêtes et d'Analyses, para.

4). The French Civil Aviation Code, Article L 722.2, also protects sources to the REC from disciplinary and administrative sanctions. This code stated, “any person involved in an incident, which spontaneously and with no delay reports it to the BEA, is protected from any disciplinary or administrative sanction, except in case of deliberate or repeated offenses to safety rules” (Bureau d'Enquêtes et d'Analyses, sect. 1). Anyone interested in enhancing aviation safety may access the REC database (GST, 2001b). According to GAIN’s GST, French commercial airlines will eventually participate in the REC.

The BEA Aviation Accident-Incident Database is the French government’s official database for the mandatory reporting of aviation accidents and incidents required by regulation and by investigations made through BEA. Access to the database is restricted to official government agencies. The BEA regularly publishes public, summary reports of safety analyses based on data and information contained in the database. The BEA Aviation Accident-Incident Database will eventually integrate with the ECCAIRS’s database and other international aviation safety information sharing systems (GST, 2003).

France’s DGAC Incident Reporting System and Quality Assurance Program for Air Traffic.

The French government office of the Directorate-General of the Civil Aviation (DGAC) manages two mandatory aviation safety information sharing systems. The DGAC Incident Reporting System and Quality Assurance Program for Air Traffic Services require the reporting by pilots and air traffic controllers of “any incident that has/might have compromised the safety of flight” (GST, 2001b, DGAC). The anonymity of individuals referenced in reports submitted to and shared by the DGAC “must be respected" (GST, 2001b, DGAC). DGAC submits aviation safety information to the European Coordination Center for Aviation Incident Reporting Systems (ECCAIRS). ECCAIRS distributes the DGAC information to European Union member states as a structured ICAO ADREP database and taxonomy.

Nordic Group's NORDAIDS.

Sweden, Norway, Finland, Denmark, and Iceland have established NORDAIDS as a multi-national aviation safety information sharing system. NORDAIDS collects mandatory aircraft incident and accident information shared between Nordic countries, as well as Canada, Germany, and the U.S. (GST, 2001b).

NORDAIDS does not protect its membership from public disclosure. However, the GST has qualified participation interest as "high with few legal actions from findings in investigations" (GST, 2001b, NORDAIDS). NORDAIDS structures its data to ICAO ADREP standards.

United Kingdom's CAA Mandatory Occurrence Reporting Scheme (MORS).

The U.K. CAA Mandatory Occurrence Reporting Scheme (MORS) is a mandatory reporting system that collects information regarding "all safety hazards or potential hazards involving U.K. registered aircraft or aircraft in U.K. airspace" (SRG, 2001, Safety Data). Identities of sources to MORS have limited protection under the Regulation 9 of the U.K. Civil Aviation Authority Regulations 1991 (GST, 2000a). Among other defined entities and individuals, Regulation 9 specifies that the public and other interested parties may access the identity of flight crewmembers and aircraft operators (U.K. Civil Aviation Authority, 1991). At the time of this review, it is unknown what affect the aforementioned U.K. FOIA 2000 will have on MORS.

U.S. Government Sponsored Aviation Information Sharing Systems

The U.S. government facilitates several airline and general aviation information sharing systems. These systems vary from mandatory airline safety information tracking and analysis programs to voluntarily sourced general aviation databases. The U.S. government does not protect aviation safety information sharing systems stipulating mandatory collection of data or information from disclosure (GST, 2001a). Within the U.S., the FAA FAR Part 193 Rule protects disclosure of sources for aviation safety data and information voluntarily collected through an FAA approved program (Simmons & Forrest, 2005).

Aviation Safety Hotline.

The U.S. FAA sponsors the voluntary Aviation Safety Hotline as a continuously operating, telephone-based reporting system. The system is unique in that reporters may select to remain anonymous, provide their name under confidential protection, or provide their name without requesting confidentiality (GST, 2003). The U.S. Privacy Act of 1974 protects the confidentiality of reporters to the Hotline (U.S. F.A.A., Office of System Safety, 2003). Anyone may report aviation safety related information to the Hotline using a toll free telephone number.

The Hotline provided real-time FAA response to safety issues. Reporters have submitted information that has led to flight cancellations and the testing of pilots that appeared not to be sober (GST, 2003). Other types of reported information include "improper record keeping, non-adherence to procedures, [and] unsafe aviation practices" (U.S. F.A.A., Office of System Safety, 2003, para. 1). The FAA plans to re-introduce the Hotline as an Internet and telephone-based reporting system.

Aviation Safety Institute (ASI).

In 1973, John Galipault (Aviation Safety Institute, 2002) of Ohio State University founded the Aviation Safety Institute. Galipault established one of the earliest known aviation safety information sharing system (S. Niedek, personal communication, September 5, 2002). The ASI safety information sharing system initially held source identification confidential and used collected data to mitigate future aviation accidents and incidents (Aviation Safety Institute, 2002). Galipault (1989, Communications Problems?) established ASI on the philosophy that, "Communication is key to the identification and elimination of aviation safety hazards." Galipault added that successful proactive safety information sharing systems require the (a) observation of hazards, (b) communication of hazards to individuals or entities that can mitigate or solve the dangers, and (c) motivation for solving the hazards.

During the early 1980s, the ASI safety information sharing system evolved into the Aviation Special Interest Group (AVSIG) (Aviation Safety Institute, 2002). AVSIG is recognized as the "world's oldest international computer forum community" (Aviation Safety Institute, About AVSIG.com). ASI's AVSIG is a privately held organization administered over the Internet via the CompuServe network. Access to AVSIG varies from free services to fee paid options. AVSIG is both a global information sharing system and network of practice where members can exchange information regarding aviation safety and many other related topics. AVSIG does not protect the identities of its membership (CompuServe, 2002).

Air Transportation Oversight System (ATOS) and Safety Performance Analysis System (SPAS).

The U.S. Air Transportation Oversight System (ATOS) and Safety Performance Analysis System (SPAS) are initiatives designed and used by the FAA to track and analyze airline safety and inspection issues specific to individual carriers. Participation by carriers within the ATOS and SPAS systems is mandatory for large U.S. airlines (GST, 2001b). Access and use of information collected by ATOS and SPAS is restricted to the U.S. government and airlines participating within the systems. SPAS collects and analyzes data and information previously collected by other aviation information sharing systems (Duquette, 2002).

NASA and FAA Aviation Safety Reporting System (ASRS).

In 1976, NASA and the FAA implemented the Aviation Safety Reporting System (ASRS). ASRS is a voluntary aviation information sharing system that provides sources to the database confidentiality and protection from punitive action (U.S. National Aeronautics and Space Administration, 2000). NASA maintains administration of ASRS as an agency independent of the FAA. Charles Billings, Chief Scientist of NASA AMES (retired) designed, implemented, and managed ASRS.

Prior to ASRS, FAA aviation safety information sharing initiatives failed since the FAA is “both the maker of the law and its enforcer” (Orlady & Orlady, 1998, p. 402). It was determined that NASA’s administration of the ASRS system would increase trust by stakeholders to the aviation community (Sullivan, C., 2001). The FAA will not seek civil penalties (i.e., monetary fines) or certificate action against sources to ASRS, provided the reported incident or unsafe operation was inadvertent, non-deliberate, did not involve criminal actions, and not related to an accident. Furthermore, sources contributing to ASRS must not have any prior FAA action regarding violations within the previous five years of the date of the occurrence or incident reported. ASRS accepts reports and provides immunity against civil penalties and pilot certification suspension or revocation if the report is received within 10 days of the occurrence (NASA, 2000).

ASRS holds all source and identity information as confidential. According to NASA, more than “300,000 reports have been submitted … and no reporter's identity has ever been breached by the ASRS” (2000, Confidentiality). NASA removes or generalizes data elements, such as organizational names, dates, times, and other information that may infer identity (Simmons & Forrest, 2005). Billings (1998) recounts an effort made through the FOIA by parties seeking to identify various contributors to ASRS involved in near mid-air collisions. To help insure the integrity of ASRS, the U.S. Congress intervened to protect the identities of the sources to the reports eventually released.

The ASRS database has been recognized as a U.S. national resource and as “the world’s single best source of data on human operator error” (Rosenthal, 2002, Aviation Safety). According to Billings (1998), the success of ASRS stems from a sincere interest by contributors to improve aviation safety, rather than the prospect of immunity.

Contributors trust ASRS to use data and information to solve aviation safety related problems.

National Transportation Safety Board (NTSB) Aviation and Incident Database.

The National Transportation Safety Board Aviation and Incident Database is the official U.S. repository of aviation accident data and causal factors (U.S. Department of Transportation, 2002). The NTSB is an independent Federal government agency responsible for investigating civil aviation accidents and incidents within the U.S. Factual reports issued by the NTSB are available for public disclosure. Users of the database include airlines, media, academia, and lawyers (GST, 2001b, NTSB).

Near Midair Collision System (NMACS), Aviation Safety Action Programs (ASAP), and Flight Operational Quality Assurance (FOQA).

Voluntary aviation safety information reporting systems supported by the U.S. government include the Near Midair Collision System (NMACS), Aviation Safety Action Programs (ASAP), and the aforementioned Flight Operational Quality Assurance programs. As an information sharing system, NMACS collects and analyzes data and information related to in-flight incidents where aircraft have operated within unsafe distances from other aircraft. Primary sources for data collected by NMACS are pilots and FAA Flight Standards Inspectors (GST, 2001b). According to the FAA, "NMAC data is available for public disclosure except for pilot personal information, inspector comments, and causal factor information (T. Payne, Personal Communications, September 17, 2002).

ASAP is a formal safety partnership entered between the FAA and individual participating U.S. airlines (Simmons & Forrest, 2005). Data and information collected from each ASAP partner is used to correct or mitigate universal problems within the airline industry. Users of ASAP data and reports consist of air carriers, the FAA, and various professional organizations (GST, 2001b). According to the FAA, airlines electing to participate within ASAP are responsible for establishing "programs with compatible data collection, analysis, storage, and retrieval systems" (U.S. F.A.A., 2000d, p. 1)

The ASAP initiative solicits the voluntary reporting of safety issues by airline employees, "even though they may involve an alleged violation of … Federal Regulations" (U.S. F.A.A., 2000d, p. 1). The ASAP agreement provides sharing incentives that under specific conditions are limited to non-punitive action (GST, 2001b). The FAA will take administrative action against sources revealing their involvement in "possible criminal activity, substance abuse, controlled substances, alcohol, or intentional falsification" (U.S. F.A.A., 2000d, p. 1). Administrative action is limited to the issuance of a warning notice or letter of correction by the FAA. Source information to ASAP reports issued to participating airlines for corrective action are de-identified (GST, 2001b).

ASAP offers individuals providing safety or security related information protection by the FAA from legal action or punishment by employers. However, this protection is warranted providing that the FAA's discovery of information related to the report is based on "sole-source" ASAP report(s) (U.S. F.A.A., 2002e, p. 4). The FAA may proceed with administrative or legal action if evidence existed that enforcement would have been implemented regardless of the existence of a related ASAP report.

The ASAP program includes a "voluntary disclosure policy" that allows regulated participating airlines the ability to report certain regulatory violations without retribution. These reports must include a plan by the airline for self-corrective action related to preventing the reoccurrence of violation (U.S. F.A.A., 2002e).

In addition to ASAP, the previously described FOQA voluntary reporting system provides protection against FAA enforcement. Enforcement protection extends to airlines that submit to the FAA a FOQA Implementation and Operations Plan. This agreement requires participating airlines to "take corrective action for adverse safety trends identified in FOQA data, and … that the FAA will have access to de-identified FOQA information on the air carrier's premises to verify the effectiveness of such action" (GST, 2001b, FOQA). Future applications of FOQA will include developing standards that will enable the integration of ASAP data and information (Orlady & Orlady, 1998).

Operational Error and Deviation System (OEDS).

Similar to PDS is the FAA Operational Error and Deviation System (OEDS) mandatory reporting system. OEDS collects data and information related to ATC and pilot actions that resulted in safety or operational violations (GST, 2001b). The OEDS system does not de-identify sources, and has access policies similar to PDS. The U.S. FAA Office of Aerospace Medicine (1999) has used the database to conduct research related to shift work demands and human error. PDS also develops and tests tools for the automated generation of information, or "information mining," related to safety information databases (Brown, Parrish, Vrbsky, Dixon, & Gainer, 1999, Introduction).

Pilot Deviation System (PDS).

The U.S. government also supports various aviation information sharing initiatives designed to investigate specific safety issues, or to test the feasibility of information technology used to collect and analyze aviation safety information. The FAA Office of System Safety's Pilot Deviation System collects mandatory information used to determine and describe if actions made by pilots were in violation of FAA regulations (GST, 2001b). Government agencies, the media, and other entities may identify, access, and use source information contained in the PDS (GST, 2001b). Principal contributors to PDS are air traffic controllers (ATC) and FAA Flight Standards investigators. The PDS program also serves as a test bed for information technology and analytical tools used to access and analyze data and information contained within the database (Institute of Transportation Studies, 2000).

Service Difficulty Reporting System (SDRS).

Established in 1966, the Service Difficulty Reporting System is a mandatory and voluntary reporting system for safety issues related to in-service or operational problems. Any aviation industry stakeholders may voluntarily report the failure of a system, component, or part of an aircraft. The FAA maintains the identity of reporters submitting voluntary information as confidential (U.S. F.A.A. Flight Standards Service, 2003). Reporting is mandatory for various FAA certified air carriers and commercial operators. Reporters use the Internet to submit reports. The U.S. FAA shares SDRS data and information with other countries such as Canada and Australia (GST, 2003).

Other Government Sponsored Aviation Safety Information Sharing Systems

Australian Transport Safety Bureau (ATSB) and Confidential Aviation Incident Reporting Program (CAIR).

The Australian Transport Safety Bureau (ATSB) requires the reporting of aviation accidents and incidents within Australia (GAIN, 2000a). Identification of sources contained in the ATSB database are not protected from public disclosure unless that information is contained in various documents protected by the 1991 Commonwealth Freedom of Information Act. The Air Navigation Act of 1920 also provides limited protection to the identity of individuals and CVRs within Australia (GAIN).

The ATSB also administers the Confidential Aviation Incident Reporting Program (CAIR). CAIR accepts reports from all sources concerned with aviation safety (Sullivan, C., 2001). CAIR maintains the confidentiality of its sources. The CAIR system collects only the voluntary reporting of aviation incidents and safety concerns not held mandatory by the ATSB. The ATSB deletes all personal information submitted through CAIRS (Australian Transport Safety Bureau, 2002).

Canadian Aviation Information Sharing Systems.

The Transportation Safety Board of Canada (TSB) administers the Aviation Safety Information System (ASIS). ASIS is a mandatory and voluntary reporting system containing data and information related to aviation accidents and various types of incidents (GST, 2001b). Mandatory reporting includes all accidents and some incidents depending on the category and weight of aircraft. ASIS accepts any type of aviation safety related information voluntarily reported. In most cases, information contained within ASIS is subject to public access (GST, 2001a). Information contained within ASIS and other Canadian government sponsored transportation safety information systems have limited protection from public disclosure. The Canadian TSB Act protects the disclosure of sources to "certain sensitive information such as witness statements, medical information, CVRs and other personal information" contained in ASIS (GST, 2001a, Public Disclosure).

ASIS and other information sharing systems of the Canadian government are subject to the Access to Information Act (ATI). Similar to the U.S. FOIA, the ATI "gives Canadian citizens as well as people and corporations present in Canada the right to have access to information in federal government records" (Canada, 1998, The Access to Information Act). The ATI excludes the disclosure of information that may cause harm or damage to national security, law enforcement, and trade secrets (Canada, 1998).

The TSB also sponsors the confidential and non-punitive SECURITAS reporting program (Sullivan, 2001).[11] SECURITAS collects voluntarily submitted safety information related to marine, rail, and air modes of transportation (GAIN, 2001b). According to the Transportation Safety Board of Canada (Canada, 2001), the purpose of SECURITAS is to identify and help mitigate widespread safety deficiencies. Sources to SECURITAS are "Anyone with a safety concern, including those who wish to have their identity protected" (GAIN, 2001b, SECURITAS). The identity of contributors to SECURITAS is confidential and deleted from any TSB published reports (Canada, Transportation Safety Board, 2001). SECURITAS does not protect the identity of individuals reporting regulatory infractions or illegal activities (TSB, 2001).

---

[11] SECURITAS become the successor of the Canadian Confidential Aviation Safety Reporting Program (CASRP). CASRP was terminated in 1995 (Sullivan, 2001).

The Canadian government also supports a central collecting and sharing system for aviation safety data and information. The Civil Aviation Daily Occurrence Reporting System (CADORS) collects and analyzes aviation safety information as a service to Transport Canada's senior management and other external stakeholders (GST, 2001b; Canada, Transport Canada, 2002). CADORS collects and processes safety information from sharing systems maintained by the TSB, NAV Canada, airports, police forces, and the public (GST, 2001b). Sources to information voluntarily contributed to CADORS have limited protection from the ATI Act (GST, 2001a).

Canadian Web Service Difficulty Reporting System (WSDRS).

WSDRS collects voluntary and mandatory information related to aircraft equipment malfunctions or other defects and failures that impede the safe operation of an aircraft. The system is voluntary for Canadian pilots operating recreational aircraft. For other operations, the Canadian Aviation Regulations require reporting. The WSDRS mutually shares information with Australia and the U.S. The WSDRS holds confidential the identity of individual reporters or affiliated company information (Canada, Transport Canada, 2003d). WSDRS allows air carriers, aviation organizations, manufacturers, and aircraft owners to search its database (GST, 2003).

Finland's VASA.

Since 1985, the Finnish Flight Safety Authority (FFSA) has been collecting aviation safety information from Finnish airlines, commercial aviation operations, Finnish government agencies, individual pilots, aviation clubs, and other sources voluntarily contributed. VASA is a mandatory reporting system for all known aircraft accidents, incidents, and other safety issues. Data and information collected in VASA is not confidential. Since 2002, ECCAIRS initiated a gradual replacement of the VASA program (GST, 2003).

ICAO Accident and Incident Data Reporting (ADREP).

ICAO sponsors the Accident and Incident Data Reporting (ADREP) program on behalf of member states. The ADREP program requires all ICAO states to report information on investigated accidents and serious incidents that involve aircraft of specified maximum take-off weights. Data and information sent to ADREP using Annex 13 standards and policies require the protection of confidentiality. ICAO analyzes information contained within the ADREP relational database and distributes the results of those analyses through bi-monthly reports to various agencies within contracting states (GST, 2001b). ICAO formally recommends all contracting states participate in GAIN as well as ADREP as a way to reduce aviation accidents through the analysis and timely exchange of information (Pereira, 2002).

Japan's Aviation Safety Information Network (ASI-NET).

The Aviation Information Safety Network is an internal airline safety information sharing system administered between various Japanese air operators. ASI-NET is a voluntary information sharing system that maintains complete privacy to source information. In addition to ASI-NET, Japan's Aviation Bureau requires the reporting of all accidents and incidents. With the exception of provisions made in Japan's Information

Disclosure Law, the Aviation Bureau provides no protection from public disclosure (GST, 2001a). The Information Disclosure Law restricts access to information that is determined to pose harm or financial loss related to a business, state agency, or international relations (Japan, Information Clearinghouse, 2002).

New Zealand's Aviation Safety Monitoring System (ASMS), Independent Safety Assurance Team (ISAT), and Information Collected Anonymously and Reported Universally System (ICARUS).

The New Zealand Civil Aviation Authority (CAA) facilitates the Aviation Safety Monitoring System (ASMS). ASMS is a mandatory reporting program that tracks data and information related to all New Zealand aircraft accidents and serious incidents. The CAA applies the previously described Just Culture policy to all sources held within the ASMS database. Just Culture protects the confidentiality of sources to ASMS, except in cases of extreme recklessness or the deliberate contribution of false information. According to the GST (2001b), the ASMS program has motivated the New Zealand aviation industry to reveal and discuss their safety failures with the CAA.

The CAA may also protect the identity of individuals through New Zealand's Official Information Act and Privacy Act (GST, 2001a). This act enables the protection of privacy by demonstrating "good reason" (Communications Law Centre, 2000, Reasons for Withholding) for the restriction to access information contained within ASMS. In relation to ASMS, a good reason for restricting access to source information is that it may influence or deter the supply of similar information from existing or future contributors (GST 2001a).

Issues related to confidentiality and financing frustrated initial efforts by the New Zealand government to establish aviation safety information sharing programs. In 1988, the Independent Safety Assurance Team (ISAT) established a confidential aviation safety information sharing program funded by the New Zealand Airways Corporation. In one instance, the Corporation became upset with a safety report issued by ISAT and demanded to know the identity of the reporter. An analyst for ISAT released the identity to the Corporation. Subsequently, ISAT failed when "industry lost confidence in the system after an analyst knowingly released the name of a reporter to the regulator" (Sullivan, C., 2001, pp. 4-5).

In 1995, New Zealand reestablished ISAT as an independent, privately held company known as the Information Collected Anonymously and Reported Universally System (ICARUS). Initial funding from the New Zealand Airways Corporation and private individuals failed to sustain the organization. The Corporation requested that the New Zealand aviation industry fund ICARUS. Former head of ICARUS, Ross Ewing, explained that this strategy also failed when the New Zealand aviation industry demanded ownership of ICARUS and access to the identities of those contributing information to ICARUS (R. Ewing, personal communications, May 3, 2003). Ewing stated that ineffective funding and ownership and legal issues, rather than any breach of confidentiality caused the termination of ICARUS in 1998. Lessons learned from ICARUS regarding aviation safety information sharing systems establish the need for "support from the regulator (without attempts to identify reporters), industry associations, and understanding the culture of the country" (Sullivan, C., 2001, p. 5).

South African Aviation Safety Council (SaasCo) and the Confidential Aviation Hazard Reporting System (CAHR).

The South African Aviation Safety Council (SaasCo) was a nonprofit organization that managed the national Confidential Aviation Hazard Reporting System (CAHR) for the Republic of South Africa (RSA) (EUCARE, 1995). The Civil Aviation Authority of the RSA provided financial support for SaasCo. Various printed reports distributed safety information collected by SaasCo's CAHR system (EUCARE, 1995). The RSA terminated SaasCo due to a lack of funding (Sullivan, C., 2001).

Concerns of Aviation Safety Information Sharing Systems and Airline Operations of Less-developed Countries (LDCs)

All known examples of aviation safety information sharing systems are initiatives underwritten by First World nations. The U.S. government and European Community expressed concern over the ability to access, track, store, and disseminate safety issues related to airline operations within Less-developed Countries (LDCs) (Henrotte, 1997; Murphy, 1997). By 1996, LDCs operated 12% of the world's airline fleet. Yet, these airlines accounted for 10 times the total number of fatal accidents occurring within the global airline industry (Murphy, pp. 13.4-13.5).

Murphy (1997) believed that requiring LDC governments to regulate and train their pilots to more-developed country standards would help to bring the safety level of global airline operations to the desired goals expressed in GAIN. In contrast, Henrotte (1997) noted that EURO-GAIN initiatives should include ways to stimulate cooperation of LDCs that would enable the collecting and sharing of LDC aviation safety operations. The difficulty in both strategies is to develop international legislation to which Third World nations would agree. Legislation and regulatory agreements needed to enforce reporting systems used to assess and mitigate aviation safety problems do not exist in Third World nations. Currently, the FAA requires all international flights operating to and from the U.S. to agree to inspections and regulatory procedures. The European Community maintains a policy of inspections of Third World airlines when suspicion of safety concerns or other operational procedures arise (Henrotte). Presently, no common policy exists to encourage sufficient trust to allow information sharing between First and Third World countries.

Knowledge Management and the Diffusion of Safety Information – Other Domain Case Examples

Non-punitive aviation safety information sharing programs can provide increased understanding of how the aviation system works (Simmons & Forrest, 2005). These programs often reveal unknown problems related to safety within the aviation industry (Orlady & Orlady, 1999). Despite the complexities and challenges of implementing KM processes to create non-punitive safety information sharing systems, many domains other than the aviation industry have implemented similar programs. The following cases provide examples of some of those programs and their respective challenges relevant to disseminating safety information.

The Medical Industry – Error Reporting

The sharing of information related to medical errors across communities within the healthcare industry is an essential process contributing to patient safety (Cohen, 2000; Uribe, Schweikhart, Pathak, Dow, & Marsh, 2002). The U.S. Institute of Medicine (IOM) identified medical errors as a cause for approximately 44,000 to 98,000 deaths in U.S. hospitals each year. The IOM defined medical error as the failure of planning or implementing actions as intended. The greatest impediment to mitigating medical error identified by the IOM is the lack of data and information describing previous errors. The U.S. and other national medical industries have identified, studied, and modeled the advancements made by the aviation industry in developing safety information sharing systems (Anderson & Webster, 2001; Barach & Small, 2000; Helmreich, 2000). Significant barriers to the diffusion of medical error information are similar to barriers to the sharing of airline safety information (Barach & Small). As in the aviation industry, medical personnel fear punitive actions for reporting medical errors (Uribe et al.).

In response to the need to share and analyze medical errors, various countries and medical organizations, have established reporting programs. According to the Institute of Safe Medication Practices (ISMP) (2003), Canada, Hong Kong, Israel, Spain, Sweden, the United Kingdom, and the United States have established various forms of international medical error reporting programs. Within the U.S., ISMP, along with the United States Pharmacopoeia, manage the Medication Errors Reporting Program (MERP). MERP is an independent and “confidential, voluntary medication error reporting program” (Cohen, 2000, p. 728). The MERP database collects approximately 100 reports per year. Each report provides an opportunity to submit detailed information regarding the reported error. The MERP system permits anonymous reporting and protects the confidentiality of identities voluntarily submitted in each report. The quality analysis of data and information contained within MERP has helped to mitigate the reoccurrence of various medication errors (Cohen).

In contrast to MERP, the U.S. Safe Medical Act of 1990 established a mandatory reporting system designed to collect data and information from healthcare facilities and manufactures. The Safe Medical Act of 1990 system requires the reporting of illness or injury regarding the failure or misuse of medical equipment. According to Cohen (2000), this system has been unsuccessful in collecting reports since it rarely takes any action without a significant number of similar reports and makes little attempt to analyze and disseminate the data or information collected.

In an attempt to overcome the deficiencies of mandatory medical reporting systems, the U.S. medical industry is constructing a new voluntary reporting system based on an existing aviation safety reporting system. In 2000, the U.S. Department of Veterans Affairs (VA) formed an agreement with NASA's Aviation Safety Reporting System (ASRS) to develop the Patient Safety Reporting System (PSRS) (2003). The PSRS is a voluntary, confidential, and non-punitive program available to all employees for reporting events and concerns related to patient safety (PSRS). PSRS duplicates the highly successful ASRS model for aviation safety information reporting. Since its inception, ASRS has protected the identity of over 500,000 safety reports from disclosure. The goal of PSRS is to discover and learn about patient safety related issues within the VA health care system. The Veterans' Benefits Act of 1997 established sources and information reported to PSRS as confidential and privileged information.

In contrast to ASRS, PSRS does not promise immunity to those reporting information to the system (Andrus, Villasenor, Kettelle, Roth, Sweeney, & Matolo, 2003). Andrus et al. stated that a “medical error-reporting system without absolute anonymity and nondiscoverability that does not ensure absolute immunity from punitive results for the reporter will not succeed (p. 916). Information reported to PSRS is considered confidential, privileged, and under NASA’s direct control. However, Andrus et al. feared that the Freedom of Information Act and other legal processes could release aggregate data contained in PSRS. Furthermore, proposed government information policies are advocating the deliberate and regular release of medical information beginning in 2008. These future policies will only protect patient privacy. Andrus et al. described these factors as critical barriers to the future success of medical error reporting systems.

Cohen (2000) has described voluntary and confidential reporting systems within the medical industry as more successful in collecting error information than mandatory reporting programs. He explained that physicians provide detailed reports when not fearing retribution resulting from disclosure. Medical personnel contributing to voluntary reporting systems are also more likely to contribute information describing the potential for error or “near misses” (Barach & Small, 2000, pp. 761-762). In agreement with Cohen, the Oncology Nursing Society (ONS) (2002) has recommended that voluntary, confidential, and non-punitive medical reporting systems designed for the improvement of patient safety become established as a national standard.

The Oncology Nursing Society (2002) also recommended that Federal protections from disclosure also be extended extend to those contributing information. However, the

ONS believed that Federal law should not supersede state evidentiary laws that provide greater protection from disclosure. Barach and Small (2000), Cohen (2000), and Uribe et al. (2002) have identified significant issues related to public disclosure and acting as barriers to reporting medical errors or near misses:

1. Medical practitioners are fearful of legal, administrative, or economic retribution for reporting errors or near misses.
2. Medical practitioners tend to report less useful information since detailed information may divulge their identity.
3. Medical practitioners fear that reported information will influence their professional reputation.
4. Medical practitioners fear that reported information will influence how superiors evaluate their professional abilities.
5. Medical practitioners fear blame by co-workers and management for reporting errors, regardless of their level of involvement in the error or near miss.
6. Medical practitioners fear that reporting errors or near misses may violate cultural norms and create a lack of trust with and between their colleagues.

Barach and Small (2000), Cohen (2000), and Andrus et al. (2003) recommended that effective safety information reporting systems should be voluntary, confidential, and offer immunity to the greatest extent possible. They also suggested that independent agencies collect information, provide expert analysis, and disseminate meaningful feedback in a timely manner to all interested stakeholders. The following list outlines other barriers identified by Barach and Small, Cohen, and Uribe et al. to the diffusion of safety information in the medical industry:

1. Extra work, time, or effort in documenting and reporting safety information.
2. Difficult availability and access to documents required for reporting.
3. Fear of identity disclosure resulting in lawsuits, blame, disciplinary action, or losing employment.
4. Fear of disclosing and reporting on other individuals.
5. Fear of crossing cultural norms.
6. Interpreting an error or near miss as unimportant.
7. Lack of understanding that an error or near miss has occurred.
8. Not understanding the usefulness of reporting.
9. Believing that reporting contributes little to improved safety.
10. Not knowing how or what information needs to be reported.
11. Not knowing who is responsible for reporting.
12. Low motivation or interest in reporting.
13. Perceiving that others are to blame and therefore have the responsibility to report.
14. Reporting system is not voluntary and confidential.
15. System does not offer immunity.
16. Reporting system does not offer feedback or analysis in a timely and useful manner.
17. Stakeholders do not learn or see results from reports.
18. Adequate funding or leadership does not exist to sustain the reporting system.

Within the U.S. medical industry, independent Peer Review Organizations (PROs) investigate reports that indicate some level of substandard care for patients covered by Medicare (American Medical Association, 2003). PROs are required to inform patients of investigations related to their medical care, but are not required to disclose the findings related to physician misconduct. Gostin (2000) offered the following description of the impact of PROs and related policy on the disclosure of medical information,

> Legal safeguards for preventing discovery of adverse event data currently exist but are imperfect. The most important of these safeguards are peer review privileges … these statutes protect data only within limited settings (eg [sic], peer review committee deliberations) and under narrow circumstances. Systems or collaborations outside the hospital or that cross state lines are often excluded from privacy safeguards. Peer review privileges are thought to be so variable and inadequate that they fail to reassure health care professionals and organizations that data will not be used in litigation against them. (para. 7)

Gostin (2000) argued that limitations on financial damages along with insurance programs should offer no-fault liability needed to protect medical practitioners from disclosure during peer review processes. In regards to all medical error reporting systems, Cohen wrote, “Practitioners do not need to be forced to report errors. They just need freedom from punishment, which is possible only with a voluntary reporting programme” (2000, p. 729). Andrus et al. (2003) added that ensured immunity requires a cultural change of self-reporting within the industry, dedicated to the welfare of patients, improvement of practice, and growth of medical knowledge. These suggestions and other reforms are unlikely in political and legal environments that sustain punitive processes as the most effective way for mitigating medical error.

U.S. Homeland Security – National Security and Safety Information Sharing

Subsequent to the September 11, 2001 attacks on the U.S., the U.S. Office of Homeland Security implemented various policies and strategies designed to improve U.S. national security and safety. The U.S. Office of Homeland Security's (2002) report, *National Strategy for Homeland Security*, established the sharing of security and safety information across state and institutional boundaries as a foundation toward improving national security.

The U.S. Office of Homeland Security described security and safety information indigenous to the U.S. as existing in "disparate databases scattered among federal, state, and local entities" (2002, p. 55). Specific to issues related to safety, the report described policies and technological infrastructure that will "disseminate information about vulnerabilities and protective measures, as well as allow first responders to better manage incidents and minimize damage" (p. 58).

Despite extensive funding of a national information infrastructure, the U.S. Office of Homeland Security identified the acquisition of incompatible technologies as a chief barrier to information sharing across and within government agencies. Various standards and technologies used within information systems have created "islands of technology – distinct networks that obstruct efficient collaboration" (U.S. Office of Homeland Security, 2002, p. 56). In addition to technological concerns, the report also identified culture and legal concerns between government agencies as a key barrier to the dissemination of national security and safety information.

The U.S. Office of Homeland Security (2002, p. 56) addressed the aforementioned barriers by suggesting information policies (a) balance the public's right to access information with the national need for security and confidentiality; (b) balance security issues with privacy issues; and, (c) create a "system of systems" information sharing infrastructure that will support and ensure trust by all stakeholders. The report does not specify exact processes for reporting or collecting information related to national security and safety.

The U.S. Office of Homeland Security will collect and disseminate security and safety information between states, local government agencies, industry, and citizens. The U.S. government also intends to increase the sharing of security and safety information between various national governments. In 2002, the Homeland Security Information Sharing Act was passed in an effort to delineate government information polices for collecting and sharing security and safety information on local and national levels. This Act establishes the responsibility of the Office of the U.S. President to determine the declassification, processes of dissemination, and recipients of national security and safety information. Key barriers to sharing security and safety information identified in the Act are the requirements for determining the issuance of security clearances to U.S citizens, as well as other nationals. Additional barriers include the development of information systems capable of transmitting classified and declassified information to selected individuals, agencies, and geographic regions.

Information classified within the Homeland Security Information Sharing Act as "Homeland Security information" is restricted to information related to (a) threats of terrorist activity, (b) the prevention of terrorist activities, (c) the identification of suspected terrorist or terrorist organizations, and, (d) improved response to terrorist acts. The U.S. Office of Management and Budget (OMB) recommended that Homeland

Security information not include “individually-identifiable information that has been collected solely for statistical purposes under a pledge of confidentiality” (U.S. Office of Management and Budget, 2003, para. 2). The OMB requires the protection of trust and cooperation for those responding to U.S. Federal statistical surveys in order to insure the production of high quality information used in critical economic and social policy decisions.

As with all the information sharing systems discussed in this proposal, trust remains the central barrier to sharing national security and safety information. Cultural divides founded on mistrust of sharing confidential or highly secretive information exists between U.S. and other national government agencies, businesses, and the individual citizen (Lynch, 2002; Rothkopf, 2002). Steven Cooper, Chief Information Officer for the U.S. Office of Homeland Security, described that formulating policies and processes that will break down the cultural, political, and organizational barriers as the most difficult challenge related to sharing national security and safety information (Shein, 2003). In addressing these barriers, Cooper stated that the U.S. Federal government has to balance the requirement to maintain civil liberty and privacy within the U.S. with that of the needs to protect the nation through the sharing of information. Lynch (2002) provided a detailed discussion of how the Homeland Security Act of 2002 and other related U.S. Acts offer a gateway to processes that may impede cultural rights to privacy and liberty. Examples of these processes include eavesdropping, mandated reporting of information, and national identity cards.

New initiatives such as the Homeland Security Act of 2002 may also be in conflict with existing laws and government information policies that facilitate the flow of information while protecting privacy and civil liberties (Lynch, 2002; U.S. Office of Management and Budget, 2002). Examples include the various interpretations of privacy and disclosure between Freedom of Information Acts and other policies and laws concerned with national security and safety (Mendel, 2003). The following section addresses these concerns.

Other Cases of Safety Information Sharing Systems

Many industries have developed safety information sharing systems based on those used in the aviation industry (Hart, 2003; Itoh & Numano, 2002; Johnson, 2000). In addition to medical and national security entities, the energy, firefighting, and biological industries have established safety information sharing systems. These industries are developing safety information sharing systems in coordination with various government agencies and other communities of practice, such as GAIN (Hart, 2003). Common objectives for safety information sharing systems within these industries include mitigating future hazards, diffusing information across cultural and political boundaries, and providing feedback that leads to increased awareness regarding safety issues (Hart, 2003; Johnson, 2000). According to Hart, punitive actions resulting from public disclosure serve as the key barrier to sharing safety information within these industries.

The nuclear power industry has developed various types of nuclear incident reporting systems. Accidents related to nuclear energy have high political, environmental, and economical consequences. Therefore, nuclear incident reporting systems have developed a non-punitive culture for the disclosure of information related to incidents and near misses (Barach & Small, 2000). The International Atomic Energy Agency (IAEA) in association with the Nuclear Energy Agency (NEA) has established the IAEA/NEA Incident Reporting System. National government nuclear agencies are stakeholders to the IAEA/NEA Incident Reporting System. The IAEA/NEA collects individual incident reports from each participating nation and analyzes them for contributing factors that may lead to nuclear accidents. The resulting reports have a restricted distribution and contain information related only to the incident (International Atomic Energy Agency, 2003). Other nuclear power safety information reporting systems include the U.S. Nuclear Regulatory Commission's mandatory reporting system for violations of regulatory requirements (U.S. F.A.A. Office of System Safety., 1997) and the World Association of Nuclear Operators event reporting system (International Atomic Energy Agency, 2003).

The American Biological Safety Association (ABSA) and the U.S. Occupational Safety and Health Administration (OSHA) have established an alliance to share information and best practices regarding safety and biological hazards (U.S. Occupational Safety and Health Administration, 2002). The alliance is a community of practice comprised of members from both organizations that voluntarily share information and expertise regarding biological hazards.

Within the U.S., the United States Fire Administration in partnership with the National Fire Information Council, has established the National Fire Incident Reporting System (NFIRS). NFIRS enables each member state to report incidents related to fires and firefighting. The primary goals of NFIRS are to reduce the frequency of fires and related damages, death, and injuries (Worley, 1999). Worley described that the detail and time required for those contributing data and information to NFIRS as key barriers to its success. Participation in NFIRS is voluntary and determined by each state's government.

NFIRS is not a confidential reporting system. Each participating state may decide on what categories of information to collect and disseminate (U.S. Fire Administration, 2003).

Potential Solutions to Issues of Public Disclosure as Barriers to the Implementation of Aviation Safety Information Sharing Systems and the Diffusion of Airlines Safety Information

GAIN participants have identified common barriers to the GAIN initiative as a system for the diffusion of aviation safety information. Issues of privacy, standards relating to infrastructure and information, and government legislation offering protection from various forms of retribution are common in both the U.S. GAIN model and other national initiatives. Proposed and currently operating global information sharing networks all must embrace the challenge of cultural and socio-economic differences. In particular, GAIN initiative members have expressed concerns over the successful integration of airline operations pertaining to underdeveloped countries.

Issues related to public disclosure affect the implementation of aviation information sharing systems directly, as well as the diffusion of aviation safety information. The GST identified government acts, laws, special databases, special programs, and special protections as five categories of information policy commonly used to control the public disclosure of aviation safety information. Government acts include examples such as the U.S. and Australian FOIA. Laws protect certain types of information related to individuals have been used in countries such as the U.S. and Japan.

In some cases, regulatory agencies recognize special databases as protected from forced disclosure or legal action. Special programs such as the U.S. FAA Part 193 Rule also protect information from public disclosure (GST, 2001a; Simmons & Forrest, 2005).

Trust is a key factor affecting the diffusion of aviation safety information within and among aviation safety information sharing systems (Ranter, 2001; S. Niedek, personal communication, September 5, 2002). The relationship between trust and accessibility is also a potential barrier to the dissemination of safety information. Ranter has suggested that within GAIN, "information is only shared among trusted groups, thus, accessibility is, and should remain very limited" (p. 2).

Determining reporting standards and structuring aviation safety information is a highly complex and time intensive problem influencing the flow of aviation safety information. Ranter (2001) described how government agencies arbitrate disagreements between airlines and between different cultures attempting to negotiate data and information standards. Because of the time required for this process, airlines will frequently abstain from contributing information to voluntary sharing systems. Varying standards and levels of participation create databases that have significant differences in periods of time coverage and inconsistencies in meaning associated with aviation incident and accident metadata.[12]

As a recognized international agency for creating aviation standards, Ranter (2001) suggested that ICAO could improve the quality and dissemination of aviation safety data and information by creating a central database that combines and collects information from global sources. Ranter also explained how the current system of private

[12] Ranter (2001, p. 4) advised that in addition to variations of qualities and meanings in metadata, cultures have established various definitions for "aviation incident" and "aviation accident."

and independent sharing networks creates clusters of information or "silos" (Koenig & Srikantaiah, 2000, p. 32) of fragmented data and information that is difficult to locate and search. A centralized ICAO database could provide improved search interfaces, time coverage, and a standardized taxonomy describing causal factors related to incidents and accidents (Ranter).

Ranter (2001) also suggested that the primary concern for aviation sharing information systems is to provide the correct type(s) of information in a timely manner. Stakeholders often ignore disseminated aviation safety information since systems often disseminate large quantities of information at frequent intervals (Johnson, 2000). Existing aviation safety information systems often fail "to adapt information to the user's needs" (Ranter, p. 6). As a solution, Ranter proposed that the aviation industry utilize the services of information intermediaries, such as librarians or information specialists. He also suggested that aviation industry professionals be educated in ways to search and present information.

C. Sullivan (2001) also reviewed various aviation information sharing systems and identified factors that influence their implementation and success in diffusing safety information. According to Sullivan, the greatest impediment to any confidential information sharing system is "when an operator or an organization seeks to find out who submitted a … report" (Sullivan, C., p. 6). Third party actions seeking the disclosure of information held by confidential reporting systems will degrade the motivation of sources to contribute data and information to the system. The loss of trust through the intentional or accidental disclosure of confidential information will usually result in the termination of a confidential aviation safety information reporting system (S. Niedek, personal communication, September 5, 2002).

The value or effectiveness of aviation safety information sharing systems as tools for mitigating incidents and accidents are often hard to measure. Furthermore, the diffusion, analysis, application, and effectiveness of aviation safety information are difficult to track and document. Therefore, it is difficult to state that an aircraft did not have an accident because the information system's "early warning system had raised an awareness of deficiencies and action was taken to prevent such an outcome" (Sullivan, C., 2001, p. 5). The relative inability to measure success related to common aviation safety information sharing systems can impede the support and participation by industry stakeholders.

Cultural values that deter citizens from admitting errors or reporting unsafe operational procedures also restrict the implementation or adoption of aviation safety information sharing systems. C. Sullivan (2001) and Johnson (2000) warned that differences in cultural values can be a significant barrier to nations attempting to form alliances designed to share aviation safety information. According to C. Sullivan, "We live in an increasingly complex, dynamic, and globalized world: a world where responsibility and accountability are becoming more ill defined" (p. 7).

Johnson (2002) added that cultural and organizational differences create situations where airlines may reach different conclusions based on shared safety information. These false conclusions may apply to the determination of causal factors, as well as establishing new safety procedures. Furthermore, variances in organizational and cultural values often create working environments that avoid or ignore recommendations made by various information sharing systems. The core challenge to aviation safety information sharing systems within this global environment will be to develop policies, tools, and methods for successfully sharing and using information and knowledge across national and cultural boarders.

Key factors related to successful aviation safety information sharing systems have been identified by C. Sullivan as the (a) maintenance of the confidentiality of the reporter, (b) willingness of industry to use the system, and (c) provision of feedback to the reporter and industry. C. Sullivan also observed that aviation information sharing systems often fail "from a lack of commitment, funding, and the rigid application of robust procedures" (2001, p. 6). Johnson (2000) added that successful safety information sharing systems include educational processes designed to enhance awareness, usability, and benefits of the system. Well-designed systems improve safety through expert analysis of root causes. These systems also keep contributors informed of how reports are used and how effective the system is at improving safety (Johnson, 2000).

Orlady and Orlady (1999, pp. 407-408) highlighted successful non-punitive aviation safety information sharing systems as those able to offer "transactional" and "use" immunity. Transactional immunity is concerned with protecting the identity of those contributing data or information to an aviation information sharing system. Use immunity requires the protection of those accessing and using data or information diffused by the system. Therefore, a focus in this study was to identify potential solutions to the issue of public disclosure as a threat to both use and transactional immunity within and among global airline safety information sharing systems.

Public Disclosure through Government Information Policy and Freedom of Information Acts

In 1948, the United Nations (UN) issued the *Universal Declaration of Human Rights*. This document called on member states and other nations to issue policies protecting various freedoms, including the right to “seek, receive and impart information and ideas through any media and regardless of frontiers” (United Nations, 1948, Article 19). Since the issuance of these rights, various societies have established “Freedom of Information” policies and laws to uphold the right of citizens to access information held by public authorities (Mendel, 2003). Since the terrorist attacks of September 11, 2001, many nations are concerned with establishing policies or laws that control access to information related to issues of national security. International debate over Freedom of Information is a concern to the stakeholders of aviation information sharing systems. The ephemeral state of domestic and international polices regarding the right to access information versus concerns over national security threaten the confidentiality of aviation safety information sharing systems. The following examples of national policies and laws related to Freedom of Information demonstrate their impact on issues related to public disclosure and security.

The U.S. Freedom of Information Act (FOIA)

Government information is a national resource within democratic states. Access to government information and maintaining an individual’s right to privacy is essential to the operation of a democracy (Lopez, 1998). The U.S. FOIA allows a citizen to make requests for information held by the U.S. Federal government (Freedom of Information

Act, 1967). The U.S. FOIA also restricts disclosure of information categorized as a national security issue, personnel rules and practices, specific laws restricting certain information, confidential business information, law enforcement investigation records, and other minor categories (U.S. Department of Justice, 2002).

Determining disclosure policy using FOIA is a two-step process. If FOIA does not restrict access, then the Privacy Act of 1974 takes precedence. The Privacy Act of 1974 restricts access to any information that is contained in a "system of records" (Gellman, 1996, p. 144). According to Gellman, the records restricted to access consist of information retrieved by name, social security number, or other personal identifier. The problem with these criteria is that personal information is contained in other government records accessed using other identifiers. Another problem is that Federal agencies have been able to avoid the process of complying with the Privacy Act of 1974 by deliberately structuring their databases to avoid categorization as a system of records (Gellman).[13]

FOIA is also in conflict with freedom of information laws held at the state level (Gellman, 1996). In some states, personal information restricted by FOIA can be accessed using local government-held records (Gellman). Additionally, FOIA is in conflict with policy administered by foreign national governments covering retrieval rights to personal information (Gellman).

FOIA policy was legislated to reduce the chance of "a clearly unwarranted invasion of personal privacy" (Gellman, 1996, p. 147). According to Burger, the FOIA's primary purpose was to recognize "the polity's right to know, within specifiable limits,

[13] With the passage of the USA Patriot Act (2001), the strategy of restructuring databases to avoid classification as "records" may no longer be a viable option. The USA Patriot Act sanctions court ordered access to any tangible item, in addition to data or information classified as records.

what the government is doing" (1993, p. 71). This dichotomy has contributed to FOIA as a "conflicting policy" (Relyea, 1996, p. 184).

To overcome and clarify part of this conflict, Attorney General Janet Reno issued a memorandum regarding FOIA and restricting the disclosure of government information. Reno's memorandum stated that Federal agencies must first assume a presumption of disclosure. No longer could agencies withhold information where there has been "a substantial legal basis for doing so" (Reno, 1993, para. 2). The memorandum also encouraged administrators to make discretionary disclosures of protected information that will not cause harm to an interest once released. Critics have argued that this leaves FOIA policy in the hands of the U.S. Department of Justice. Advocates believe that this policy encourages a more open FOIA environment as applied to individual Federal agencies (Relyea, 1996).

In addition to policy issues, considerable controversy exists over the implementation of electronic infrastructures as it relates to FOIA (Relyea, 1996). Information stored in electronic format is subject to FOIA. Differences in technological standards have caused barriers to individuals exercising rights granted by FOIA. Incompatible network technologies have had a detrimental affect "on reasonable responses to most requests for electronic records" made available by FOIA (Relyea, p. 189).

The U.S. FOIA and national security.

U.S. President George Bush further modified FOIA in October 2001 by issuing the Ashcroft FOIA Memorandum. This policy supported the full compliance by the U.S.

government with FOIA as a tool for sustaining an open and accountable government (U.S. Department of Justice, 2002). The U.S. Department of Justice (2002) described the memorandum by stating the following,

> At the same time, it recognizes the importance of protecting the sensitive institutional, commercial, and personal interests that can be implicated in government records -- such as the need to safeguard national security, to enhance law enforcement effectiveness, to respect business confidentiality, to protect internal agency deliberations, and to preserve personal privacy. … Under this new standard, agencies should reach the judgment that their use of a FOIA exemption is on sound footing, both factually and legally, whenever they withhold requested information. The Ashcroft FOIA Memorandum also recognizes the continued agency practice of considering whether to make 'discretionary disclosures' of information that is exempt under the Act, upon 'full and deliberate consideration' of all interests involved. While it places particular emphasis on the right to privacy among the other interests that are protected by the Act's exemptions, it reminds agencies 'to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA'. (Introduction section, para. 19)

Subsequent to the September 11, 2001 terrorist attack on the U.S., the Federal government issued various proposals to strengthen the definitions of exclusions to the disclosure of information sought by the public through FOIA. U.S. policymakers have argued that increased protection of disclosure for information critical to national security and held by the private sector would help to motivate the voluntary transfer of that information to the U.S. government (Krebs, 2002). Policy strategist Alan Paller (2002) has argued against the strengthening of FOIA exemptions. However, regardless of FOIA exemptions, organizations tend to fear the sharing of data or information that, if disclosed, would embarrass the entity or cause a loss of revenue. In these cases, organizations typically share information only with those directly concerned with solving problems internal to the entity that owns the information (Paller, 2002).

In addition to strengthening exemptions to potential disclosure from FOIA, the U.S. Government also introduced measures to increase its ability to access information resulting from increased threats of terrorism. The USA Patriot Act (2001) eased restrictions on the U.S. Government for the collection of information related to criminal investigations, foreign intelligence, money laundering, and alien terrorists and victims. The Act allows the government greater latitude in tracking and intercepting communications related to cyber terrorism or other crimes. Under the conditions of the Act, government agencies can access and confiscate information technology systems in addition to data and information records contained in databases. The Act also protects the disclosure of collected data and information and identities of those helping to facilitate various titles and orders within the USA Patriot Act.

The Homeland Security Act of 2002 established the U.S. Office of Homeland Security. The U.S. Office of Homeland Security is responsible for protecting the U.S. against terrorism and other criminal acts. Title II of the Act ensures that the U.S. Office of Homeland Security may request and receive information and analysis held by any U.S. source deemed relevant to the investigation or protection of national security. Specifically, the Act provides the U.S. Government with lawful access to any information categorized as “Critical Infrastructure Information” (§ 212, Homeland Security Act of 2002). Critical Infrastructure Information includes information related to the protection of U.S. interstate commerce and public safety. The Critical Infrastructure Information Act of 2002 protects information voluntarily submitted to the U.S. Office of Homeland Security from further disclosure or dissemination through the FOIA.

U.S. Senator Leahy and other congressional members have criticized the Critical Infrastructure Information Act of 2002 of protecting *information* voluntarily submitted by the public rather than *records* (Verton, 2003). Senator Leahy expressed that using the category of information rather than records could exclude disclosure through the FOIA data and information not related to Critical Infrastructure Information. At the time of this writing, the Leahy-Levin-Jeffords-Lieberman-Byrd Restoration of Freedom of Information Act of 2003 introduced an effort to reverse shielding from the FOIA information voluntarily submitted by the public to the U.S. Office of Homeland Security (Verton).

The element of disclosure and conflicting nature of FOIA are primary concerns to the GAIN initiative and other aviation safety information sharing systems. In light of concerns regarding U.S. national security, future modifications to FOIA will most likely continue to affect the evolution and structure of GAIN and other aviation safety information sharing systems.

The United Kingdom Freedom of Information Act 2000 - Open Government and National Security

In 2000, the British Parliament passed the U.K. Freedom of Information Act 2000. Similar to the U.S. FOIA, the U.K. Act supports the right to public access of information held by the government. Due to concerns over national security, these rights do not go into effect until 2005 (Campaign for Freedom of Information, 2001). The Act requires the government to confirm, deny, and disclose information. However, public access is limited to various agencies and categories of information. For example, the public may not access security, military, and intelligence information (Wadham & Modi, 2003).

The U.K. Freedom of Information Act is a step toward a policy of “Open Government” (Wadham & Modi, 2003, p. 7). In 1997, the Open Government policy attempted to improve citizens’ confidence in the U.K. government by taking steps to remove secrecy. However, the U.K. Freedom of Information Act 2000 has created more debate than confidence, since the Act contains 36 restrictions to information access and allows government ministers to modify terms of disclosure in the interest of national security (Weir, 2002). At the time of this review, it is unknown what affect the U.K. Freedom of Information Act will have on aviation safety information sharing systems.

Other National Freedom of Information Acts

Various human rights organizations, in cooperation with the UN, have advocated and issued policies supporting the global adoption of FOIA legislation. Countries such as Bosnia-Herzegovina, Canada, the Nordic Region, Romania, Slovakia, South Africa, Zimbabwe, Mexico, Peru, Japan, Thailand, and India have established various FOIA initiatives. Despite the institution of FOIA as a fundamental right by the UN, many nationalities have failed to establish FOIA legislation. In nations supporting FOIA policies and laws, related standards and processes are often inconsistent and debated in each of these societies (Mendel, 2003).

Many countries adopting FOIA legislation experience controversy similar to those in the U.S. and U.K. regarding the right of access and safeguarding national security. Mendel (2003) described how countries seeking membership in NATO must demonstrate a minimum standard of national information policy protecting secrecy and security. These requirements often conflict with established FOIA legislation indigenous to those countries seeking NATO membership.

The Australian Freedom of Information Act of 1982 (Australia, Attorney-General's Department, 2003) established the right of Australian citizens to access information held by government sources. However, information classified for security, defense, or international relations may be restricted. The Australian government also protects disclosure of information that may threaten the commercial viability of business or industry. Furthermore, processes and classifications for determining access to government held information within Australia varies depending on the laws of individual Australian States.

The New Zealand Official Information Act of 1982 enables government ministers to re-classify information that may threaten or hinder national security or defense (Mendel, 2003). New Zealand's Act allows access to information to any specified official information limited to (a) reasons for decisions made about you; (b) internal policies; (c) principles, rules, or guidelines; and (d) meeting agendas and minutes of public bodies, including those not open to the public (New Zealand, 2003).

South Africa established the constitutional right for public access to government information through the South African Protected Disclosures Act 2000 (Klaaran, 2003). The South African Act protects from disclosure information classified as secret, related to national security, or defense. The Act does include "whistleblower protection" for government employees that disclose information under specific conditions (Mendel, 2003, p. 22). Protection from employment-related sanctions for disclosures related to events such as wrongdoing or harm, criminal activity, and safety risks is included in the Act. Employees make disclosures directly to legal practitioners through formal government established procedures. Similar to South Africa, the U.S. Federal Government and various local U.S. and state government agencies, Australia, and New Zealand have established whistleblower protection policies (Martin, 2003). However, whistleblower policies are not recognized or well established in many other national governments such as Japan or Canada.

In 2001, Japan established the Information Disclosure Law permitting limited access to government information. Japan's Information Disclosure Law includes an extensive list of information classifications protected from disclosure. Government ministers in Japan have complete authority to control the disclosure of all information requested through the Law (Repeta & Schultz, 2002).

Canada's provinces and territories administer various forms of policies and laws permitting access to government information by the public (Canada, Department of Justice, 2003). As an example, Ontario's Freedom of Information and Protection of Privacy Act classifies government held information as "mandatory" or "discretionary" (Canada, Ontario Information and Privacy Commissioner, 2003). Under the Act, the public may not access information classified as mandatory. Mandatory information includes Cabinet records, third party information supplied in confidence, and information about other individuals. Each government organization within Ontario determines what information is discretionary, and whether to release information. Discretionary information includes categories such as safety, law enforcement, defense, and information related to commerce or individual organizations (Canada, Ontario Information and Privacy Commissioner).

Similar to Ontario, British Columbia's Freedom of Information and Protection of Privacy Act extends the right of the public to access information held by "public bodies" (Canada, British Columbia Office of the Information and Privacy Commissioner, 2003). Public bodies in British Columbia include provincial government, local government, and self-governing professional bodies. The public requests information directly from the public body that holds the desired information. The Information and Privacy Commissioner is an independent Officer of the Legislature, responsible for arbitrating requests for information denied by the public body. Exemptions include categories such as law enforcement, personal information, information that could harm a business, and Cabinet confidences. With the exception of personal information unique to the individual making the request, the Act does not specify categories of information that the public may access (Canada, British Columbia Office of the Information and Privacy Commissioner).

Potential Barriers to Knowledge Diffusion Within and Among Communities and Networks of Practice

Brown and Duguid stated that, "any global network has a highly varied topography" (2000, p. 144). GAIN's topography is comprised of networks and communities distinguished by common themes of practice. Structural, relational, and cognitive properties within a community or network of practice may create boundaries within and among each environment (Newell, Robertson, & Swan, 2006). Therefore, within global networks, knowledge flows according to the boundaries of those local topologies.

As a practice, KM is concerned with managing the flow of existing and new information and knowledge across boundaries created by various topologies (Sanchez, 2006). According to Spender (2000), KM's mission is to apply processes that disseminate tacit knowledge as a public good across the boundaries formed by various topologies. This assessment does not imply that KM should focus on the removal of boundaries. Wensley and Verwijk-O'Sullivan stated that, "New knowledge will not be created if there are not barriers to rail against" (2000, p. 118). They suggested that KM is a tool to create and manage boundaries that affect the transfer and diffusion of knowledge.

Barriers to knowledge diffusion within and across various structural, relational, and cognitive topologies are wide-ranging, inter-related, and often specific to the environment examined. However, various studies have delineated common themes related to boundaries that may have an affect on the dissemination of knowledge within and among various settings (Davenport & Prusak, 2000; Murray, 2000). Davenport and Prusak have qualified barriers to the dissemination of knowledge as “frictions” since "they slow or prevent transfer and are likely to erode some of the knowledge as it tries to move through the organization" (p. 96). In this case, Davenport and Prusak identified barriers such as trust, culture, spatial factors, and human perceptions in relation to the business or organizational environment. However, authors such as Morey, Maybury, and Thuraisingham (2000) and Despres and Chauvel (2000a) have provided evidence that these barriers are also common to communities of practice, networks of practice, and other knowledge-based environments.

Knowledge environments are "quasi-autonomous, partly self-organizing, [and] partly constrained to an evolutionary trajectory" (Spender, 2000, p. 165). The self-organizing nature of knowledge and communities and networks of practice improves the transfer and diffusion of existing and new knowledge (McElroy, 2003). McElroy suggested that KM is a process of study used to understand and facilitate the processing and diffusion of information and knowledge within these environments. Therefore, it is essential to understand the challenges and barriers related to implementing KM and facilitating knowledge diffusion.

Trust and Culture

Trust and culture are probably the most common barriers affecting the flow of knowledge (Davenport & Prusak, 2000; Ford, 2003; Sinclair, 2006). Trust derived from cultural norms is a potential barrier to knowledge diffusion. Members of a community conform to various cultural and social norms. Trust among members develops by conforming or adapting to different values, perceptions, communication structures, and goals within communities and networks. Community members will seek "common ground" in order to develop trust (Davenport & Prusak, 2000, p. 97). Davenport and Prusak highlighted common ground as the ability of communities to create opportunity for personal communications through activities such as educational programs, meetings, and apprenticeships. As an example of these strategies, they described how the medical industry uses educational programs and meetings to share various techniques regarding surgical processes. In these efforts, medical professionals established common ground, trust, and increased motivation for learning new information and knowledge.

The common ground of cultural life relates to the ability to access information or knowledge. Those seeking the privilege of access usually seek individual membership in various communities or networks of practice (Rifkin, 2000). Access is a relational dimension between those seeking membership in the community and communities as sources “of critical ideas, knowledge, and expertise” (Rifkin, p. 5). Conditions for gaining access within cultural settings can range from acceptance of certain traditions or rights of passage to economic fees. These factors help to establish the cultural norms within communities, as well as act as potential barriers to the flow of knowledge by restricting access within each cultural environment.

Members of communities, organizations, and nations are also protective of knowledge that is indigenous to their culture or society. Cultural differences such as work ethic, physical appearance, religion, and societal competition serve as barriers to knowledge diffusion (Krogh, Ichijo, & Nonaka, 2000). Many cultures are not willing to accept or use information, knowledge, or wisdom not created within their own society. Successful knowledge diffusion often relies on the willingness of participants to communicate. Krogh, Ichijo, and Nonaka provided an example of Swiss engineers making a deliberate effort to show an interest in Hinduism with their Indian partners. In this case, the Swiss were able to increase trust and knowledge sharing with their Indian associates. Societies willing to share and show an interest in the values and beliefs of other societies tend to be more successful in removing cultural barriers affecting knowledge diffusion.

Cultural factors such as language and related standards in communication processes may also create barriers to diffusion. As a relational dimension, Rifkin observed that, “Language is the key to exploring meaning because it is the vehicle we use to communicate our thoughts and feelings to one another” (2000, p. 194). Language used within the “conversational culture” of communities of practice may serve as a barrier to knowledge diffusion if used ambiguously, to intimidate, or to exert authority (Krogh, Ichijo, & Nonaka, 2000, p. 135). Krogh, Ichijo, and Nonaka also warned that cultures advocate different rules and procedures for initializing and maintaining communication. These issues include concerns such as body language, dress codes, and who speaks first. Therefore, the ability to communicate meaning and understanding through language is essential to building trust. Personal knowledge, perception, and cognitive processing affect meaning or “sense making” ability (Snowden, 2000, p. 239). The meaning and subsequent use applied to transfer knowledge are further influenced by social considerations and related communication technologies.

Communication and Technological Standards

Building trust within communities or networks of practice also requires common standards as applied to communication infrastructure (Maier, Hädrich, & Peinl, 2006). Structural dimensions within networks of practice not only require technologies that can preserve the meaning and understanding of the communication, but also allow access to the culture participating within the network (Rifkin, 2000). Buckholtz (1995) emphasized that standards related to information and knowledge infrastructure are critical in facilitating the synergy between people and systems within communities and networks.

Cultural or economic considerations determine incompatibility between standards or the inability to recognize or adopt standards. Standage (1998) told how various governments have controlled the flow of information within and among cultures by deliberately establishing unique standards for communication systems. Desire to improve economic efficiencies through technological enhancements such as automation and increased transmission rates create incompatible technologies in communication infrastructures such as the telegraph and the Internet (Standage).

Cultures may use various political processes to issue policies that specify standards as a way to control access to information or knowledge (Strassmann, 1995). Boundaries to the flow of knowledge form when considering the costs related to managing and updating standards and related infrastructure. Strassmann illustrated how variations in the ability of cultures to afford changes in standards and related support services can severely limit the ability to acquire information. Community or network members couple economic thresholds with perceived need for the infrastructure. A common demand for standards as well as the ability to afford the infrastructure is required to facilitate the flow of information or knowledge throughout the community or network of practice (Sinclair, 2006).

Spatial, Temporal, and Economic Issues

Other potential barriers to building common ground within knowledge-based systems or environments include geography and time. Geographic distance is a well-established barrier to knowledge diffusion. Brown and Duguid stated that, "Knowledge seems to flow with particular ease where the firms involved are geographically close together" (2000, p. 163). For this reason, communities of practice that are similar tend to cluster their physical location in close proximity to each other (Brown & Duguid). Examples of this phenomenon include the high concentration of aerospace industries that have collocated in Denver, Colorado and aviation manufacturers in Wichita, Kansas. Relationships between knowledge and location has been termed “sticky local knowledge,” since tacit knowledge may become imbedded within specific cultures of a geographic location (Malecki, 2000, p. 112). Therefore, barriers that prevent locating near or within these clusters can diminish the flow of knowledge. In these situations, networks of practice form to address the barrier of geography and clustering. Networks of practice have a relational dimension that connects communities spatially distributed across varying geographies.

Time and information technology may create potential barriers closely related to relational and cognitive dimensions. A lack of time can affect the ability of individuals to learn or absorb new information or knowledge (Davenport & Prusak, 2000). The lack of time coupled with information technologies that deliver large volumes of information or knowledge can lead to cognitive (Davenport, 1997) or information “overload” (Srikantaiah, 2000, p. 16). The challenge information overload poses for the user of information or knowledge is complex. Searchers are aware of the existence and relevance of the information or knowledge sought through the way access and methods for retrieval are structured. The inabilities to search, filter, evaluate, or communicate information or knowledge efficiently may also create barriers to the dissemination of knowledge. Furthermore, once accessed and retrieved, time may limit the opportunity to “engage” (Davenport, 1997, p. 92) or apply information or knowledge.

Time, geography, and economic constraints also interfere with the opportunity for personal communication. Personal communication is possible through opportunities that allow individuals to share information or knowledge voluntarily (Davenport, 1997). Distance can diminish these opportunities by requiring extensive time or expense associated with travel or the building of networks used to bridge spatial boundaries. Swan and Scarbough described that as organizations decentralize across the dimensions of time and space, "they also lose opportunities for casual sharing of knowledge and learning induced by physical proximity" (2002, p. 11). Malecki (2000) listed airlines and government agencies as prime examples of communities affected by physical proximity and the sharing of knowledge.

Economic fees that limit access to various social structures may also inhibit the sharing of knowledge or expertise (Rifkin, 2000). The relationships between the cost of access and time for socialization are important considerations to the effectiveness of building trust within networks and communities of practice that span the barriers of time and geographical dimensions. Companies such as British Petroleum and 3M have spent considerable investment in creating meetings and fairs that enable "researchers time and space to meet and exchange knowledge" (Davenport & Prusak, 2000, p. 105).

Social Concerns

As part of socialization, Davenport and Prusak (2000) advised that social status is an important relational factor that may act as a boundary to knowledge diffusion. Perceived status within a community or network develops by ownership and access to information and knowledge. Debate exists as to whether ownership or strictly access controls status. Rifkin (2000) argued that the ability to access information and knowledge is paramount to ownership in terms of developing individual status within the community. The implication of Rifkin's observation is that knowledge tends to flow more readily to those that can gain or control access to knowledge. Rifkin has described those who control ownership or access to information as "gatekeepers" (p. 178). Gatekeepers such as America Online, Disney, and many other companies strive to control markets by purchasing the network gateways to information or knowledge (Rifkin). Davenport and Prusak (2000) argued that ownership to knowledge is the primary factor that establishes an individual's status within the community or network. In their defense of this position, Davenport and Prusak stated that those who own knowledge will have power, and "those who have power will have control over who knows what" (p. 177). Regardless of these issues, it is clear that access and ownership affect the status of those who control or own knowledge. For these reasons, status contributes to the boundaries that affect the flow of knowledge within and among networks and communities.

Social status also affects motivation for sharing and applying knowledge. Individuals and organizations are generally more willing to seek and to use knowledge held by those in positions of high social or economic status (Glaser, Abelson, & Garrison, 1983). This aspect of culture is a relational dimension between trust and status. The capacity to trust individuals, entities, or communities that have status develops from reputation and experience (Rolland & Chauvel, 2000). Anderson, Glassman, and Pinelli (1997) determined that, in situations of uncertainty, stakeholders in aviation related communities of practice would seek information that is high in quality, comprehensive, and highly relevant. In these cases, stakeholders within aviation communities of practice were more likely to seek information from nationally recognized government agencies or research institutions than from sources of a lower status. Aviation communities equate the reputation or status of recognized government agencies and research institutions with higher levels of experience. Experience evolves over time and is recognized through processes that demonstrate the application of knowledge or wisdom. Reputation develops through consistent fair dealings (Rolland & Chauvel, 2000) with individuals and other stakeholders.

Status and reputation may also act as detriments to sharing knowledge. Individuals may lose status from transferring information or knowledge that is not accurate or incorrectly used. Additionally, sharing knowledge that reveals inexperience can result in a loss of status (Davenport & Prusak, 2000). This type of cultural norm is a barrier to those seeking information – since the declared need for information is an indication of inexperience.

Geopolitical, Socioeconomic, and Government Information Policies

Individuals, entities, and communities are more likely to ask for and share knowledge when high levels of "interdependency" exist between the environments (Rolland & Chauvel, 2000, p. 321). Rolland and Chauvel described interdependency as the extent those sharing knowledge will respect each other’s commitments. This knowledge behavior suggests that higher levels of interdependency may create higher levels of trust. Different levels of interdependency may exist within and among communities and networks of practice. However, the ability of communities to build trust is largely dependent on the existing geopolitical and socioeconomic settings. A significant degree of interdependency must exist within the social infrastructure of a culture before communities and networks of practice residing within these environments can establish trust (Rifkin, 2000).

The degree of interdependency within and among cultural settings is often affected by government information policies and related socio-cultural processes. Knowledge diffusion is more effective in government and political settings that support innovation, the transfer of research and technology, and legal protection of intellectual capital (Glaser, Abelson, & Garrison, 1983). Government information policies that support the economic development of communication infrastructure may also enhance knowledge diffusion. Burger suggested knowledge diffusion as the "hallmark" objective of government information policy (1993, p. 3). Various examples of government information policies that may create boundaries to diffusion and transfer are, "scientific and technical information policy, privacy issues, literacy [public education], freedom of speech, libraries and archives, secrecy and its effects on commercial information policy and national security, and access to government information" (Burger, p. 3).

Brown (1989) and Chandler and Cortada (2000) described how early U.S. government information policies were designed to meet the needs of a society that demanded information and the diffusion of knowledge. U.S. government information policies empower citizens, create infrastructure, and transfer knowledge as a public good. These policies and related infrastructures serve as leading contributing factors to innovation, economic growth, public safety, and new social paradigms such as the advent of the Information Age (Chandler & Cortada).

Government information policies develop as a way to manage or control information. Politics can affect the dissemination of knowledge within government structures as well as every organization within a society (March, 1997). March described how those using policies governing the diffusion and transfer of knowledge gain economic and social power. Information policies and their relationship to power range in severity as applied to the control of information or knowledge. Political and organizational structures can develop policies that attempt to control all diffusion (monarchy) to systems that enable individual control over knowledge (anarchy) (March, p. 69). For instance, March stated that "information feudalism" is a model commonly found for managing information within aerospace and aviation related companies (p. 72). Under information feudalism, unit managers control the flow of information within their environment. According to March, information feudalism erodes cooperation among communities and tends to transfer inaccurate information.

Government information policies affect cultural and social barriers to knowledge diffusion (Burger, 1993). Government policies control issues such as freedom of speech, communication infrastructure, and the right to information access. These policies influence the ability of individuals, networks, and communities to socialize. The types of government information policies administered by leadership also affect the perceptions of norms and traditions that eventually help to establish cultural values (Burger). Government information policies eventually transform the cultural and social environments within communities and networks of practice. The management and translation of policies cause processes of knowledge dissemination to vary.

Proper management of government and community information policies can build trust. However, new policies that evoke change can cause fear and resistance by stakeholders. Glaser, Abelson, and Garrison advised that, "Diffusion can change the social structure of a social system" (1983, p. 147). This warning implies that changes in cultural or social processes of knowledge diffusion may threaten established common ground within a community. If not managed properly, the relational dimension between government and community information policies can cause a deterioration of trust within the knowledge-sharing environment.

Awareness and Learning

The relationship between trust, information policy, and knowledge diffusion requires proactive knowledge management. Managing knowledge-based environments must integrate policies that support developing awareness and self-interest by the stakeholders to the community or network (Ives, Torrey, & Gordon, 2000). Awareness and self-interest develop by creating learning environments. In the case of communities or networks of practice, "Learning ... is not simply a matter of acquiring information; it requires developing the disposition, demeanor, and outlook of the practitioners" (Brown & Duguid, 2000, p. 126). Learning environments provide the opportunity for collaboration, socialization, and training. These activities can help to sustain trust while administering new policies, infrastructure, or processes related to knowledge diffusion.

McElroy (2003) recommended that learning environments are best created by allowing communities of practice to “self-organize” (p. 62) around processes that facilitate the transfer and diffusion of existing and new knowledge. Management philosophies that dictate methods for knowledge processing and learning will degrade the ability of an entity to create and diffuse existing and new knowledge. Learning environments are created using self-organized processes supporting “independent individual learning, followed by group or community learning, followed by organizational adoption, followed, finally, by the integration of new knowledge into practice (McElroy, p. 152).

Developing learning environments also requires consideration for the ability and motivation of members to participate within the community or network (Ives, Torrey, & Gordon, 2000). Members of communities and networks of practice must learn the goals and directions for the policies and processes related to various knowledge sharing activities. Members are likely to resist sharing information if not made aware of why and how knowledge needs to be shared (Ives, Torrey, & Gordon). Developing motivation to participate includes learning about the processes, technologies, and cultural norms within the environment. Individuals must also perceive a mutual interest or reward for participation and knowledge sharing. Rewards can include the prospect of improved social status, economic incentives, self-esteem, or improved security.

Collaboration and Common Goals

Ives, Torrey, and Gordon (2000) suggested that knowledge sharing is greatest within and among individuals and communities that have common goals. Collaboration is required between stakeholders that are working together on a project. This interaction can cause boundaries to knowledge diffusion - especially when individuals have different cultural backgrounds, or when their personal knowledge base varies.

In addition to culture and tacit knowledge, other barriers to collaboration vary with the structure of complementary and integrative working relationships (Hara, Solomon, Kim, & Sonnenwald, 2003). Complementary collaboration subdivides and assigns required tasks to individual participants. Integrative efforts require stakeholders to share responsibility for the same tasks. Within these two structures, similarities in work style, work priorities, geographic proximity, and trust affect the willingness to collaborate and share knowledge. As with organizations, individuals are reluctant to collaborate and share knowledge when perceptions toward methodologies and processes vary, spatial barriers exists, and incentives or trust are misaligned with personal motivation for participation (Hara, Solomon, Kim, & Sonnenwald).

These relationships between collaboration and project management are of special concern to communities and networks of practice. The focus of knowledge management applied to communities and networks of practice is to stimulate the flow of knowledge "traveling on the back of practice" (Brown & Duguid, 2000, p. 126). Both those managing the boundaries to knowledge diffusion and the members to communities and networks of practice must meet this challenge.

Potential Barriers to Knowledge Management

KM addresses the development and control of new and existing knowledge within and across boundaries systemic to networks and communities of practice (Newell, Robertson, & Swan, 2006). Many factors act as barriers to the implementation and application of KM. Frictions to knowledge diffusion and transfer, as well as limitations inherent to KM methodology, affects the ability to implement KM (Murray, 2000). Despres and Chauvel underlined this problem by stating that in the case of KM, "there is neither agreement nor clarity on what, exactly, constitutes the concerted effort to capture, organize, share, transform, [or] reinvent" knowledge considered important to a network or community of practice (2000b, p. 57) (see Appendix A). Furthermore, KM often fails when processes and policies do not consider the nature of knowledge and how it relates to the social, structural, relational, and cognitive environment within a network or community (McElroy, 2003).

Kim (2003) provided an inventory of five states of organizational readiness that communities or networks of practice must address for the successful implementation of KM. Critical issues supporting KM include leadership, culture, technology, measurement, and KM process. Organizations must establish KM leadership with a high degree of authority and resource allocation. KM leadership must recognize that the sharing of information is a cultural process, and that stakeholders must be motivated to take a pro-active role in processes of knowledge diffusion. While not essential to all aspects of KM, technological infrastructure is a strategic initiative within organizations designed to support collaboration. KM processes should align with the strategic goals of the organization. In regards to KM processes, Kim emphasizes that organizations must "identify core strategic processes, critical actions, critical action personnel, and knowledge requirements, and then aggregate knowledge requirements into content centers and develop communication strategies to build awareness of KM program goals" (2003, p. 142). Leadership should implement qualitative and quantitative measurements to gauge the effectiveness and efficiencies of collaborative processes and related technologies. Kim advised that, if neglected, the aforementioned states of readiness will act as significant barriers to KM. The following sections explore various aspects related to these concerns.

Misunderstanding the Purpose of Knowledge Management

The perception of KM and related processes by stakeholders to a community or network may create barriers to implementing KM. KM is often perceived by individuals as a management practice dedicated to the control of cultural beliefs and values (Krogh, Ichijo, & Nonaka, 2000). The relationship between culture and trust interrelates with the viability of power, threatened by the sharing of knowledge (Clarke, 2000). Members of an organizational setting resist adopting KM for fear of losing control over existing boundaries that traditionally serve to control the flow of knowledge and help define the structure of power within a society. In these settings, KM is a threat to existing boundaries.

In contrast to these fears, Barquin (2003) stated that leadership should use KM to strengthen communities of practice as a way to identify and transfer best practices and knowledge across boundaries. Fears related to KM by individual members to communities of practice can be reduced by using KM to build group identities, motivate and reward individual achievement, and deliver enhanced value or utility (Hirsh, Youman, & Hanley, 2003). Building identities includes implanting social and technological processes that enhance personnel identity and membership. Examples of these efforts include meetings, Web pages, and distribution lists. Motivating participation in KM initiatives include (a) endorsing participating individuals to other members of the organization, (b) requiring participation as part of a performance evaluation, or (c) providing monetary incentives. Finally, the community of practice should make all stakeholders aware of the value or utility recognized from the KM process and each individual's involvement (Hirsh, Youman, & Hanley).

Lack of Knowledge and Resisting Knowledge Management

Implementing KM requires time and effort. Stakeholders must allocate time for learning about new KM policies and procedures. Reductions of barriers to knowledge diffusion resulting from KM also demand greater time for thinking and reasoning (O'Dell & Grayson, 1998). Members of a community or network of practice often feel threatened by KM initiatives that require a great deal of effort and policies that are perceived as a mandate to "know everything" (Davenport & Prusak, 2000, p. 97). These demands can lead to increased emotional stress and serve as a potential threat to self-image by community or network members (Krogh, Ichijo, & Nonaka, 2000).

Developing successful KM programs must include addressing factors such as ignorance by community members or organizational management, the development of training programs, and the determination of ways to motivate individuals to participate within KM-based initiatives. O'Dell and Grayson (1998) described stakeholders as often ignorant of their need for, and existence of, information or knowledge. In these cases, resistance to KM is often strong by these members to the community or network. Ignorance is a multi-faceted challenge affecting the structural, relational, and cognitive considerations of a knowledge-based environment, as well as the ability of stakeholders to adopt practices related to KM.

The need for learning environments.

Efforts related to learning and training are potential remedies for ignorance and resistance toward KM. Learning is essential to successful KM and the eventual improvement of knowledge diffusion (Krogh, Ichijo, & Nonaka, 2000; Morey, Maybury, & Thuraisingham, 2000; O'Dell & Grayson, 1998). Networks or communities create barriers to KM when stakeholders are unaware of standards, existing cultural or organizational knowledge (tacit and explicit), policies and processes, and organizational or social goals (Krogh, Ichijo, & Nonaka). KM initiatives are prone to success in environments that provide learning environments to share knowledge related to these factors. Learning environments complement KM since they support socialization, trust building, and knowledge creation.

Brown and Duguid (2000) described the importance of creating learning environments that emphasize socialization within communities of practice. Properly designed learning environments support the meaningful exchange of knowledge, the sharing of practice, and the recognition of individual identity within the community (Brown & Duguid; Wenger, 1998). Strategies that change workflow processes and geographical settings improve socialization between experienced and inexperienced members of a community or organization (Brown & Duguid, 2000). Pinelli et al. (1997) highlighted how learning environments within the aviation and aerospace industries have enhanced the transfer of tacit knowledge between engineers and research scientist. Implementing KM processes in environments that do not support learning often fail in identifying, capturing, and transferring new knowledge (Murray, 2000).

Rationalizing Goals and Incentives for Knowledge Management

Benefits for participating within networks or communities of practice are often established when the stakeholders understand the purpose or function of those structures. Authors such as Morey, Maybury, and Thuraisingham (2000) suggested that increased acceptance by stakeholders in the community or network occurs when KM meets the needs of specific missions or objectives. Under this argument, collaboration and knowledge diffusion should increase. Other writers have argued that many successful initiatives related to KM start without a specific purpose other than to stimulate the sharing of information or knowledge (Addleson, 2000; Wheatley, 1999). While not in total disagreement with defining the purpose for implementing KM, these authors suggested that the interaction and "self-organizing" relationships that evolve from KM practices are as important as the goal or rationale for the process (Wheatley, 1999, p. 87). The important point here is that KM can be justified and implemented under a wide spectrum of rationales. KM initiatives must balance this characteristic with the needs of the organization and the perceptions and motivations of the stakeholders.

The rationales justified by communities of practice to implement KM have also been identified as potential barriers to the diffusion of KM. Swan and Scarbough explained that, "knowledge pertaining to KM becomes fragmented and distributed across professional boundaries" (2002, p. 13). In their study, Swan and Scarbough provided evidence that KM is defined and molded into policies and procedures used to sustain agendas and political efforts specific to professional domains. Examples of this phenomenon include (a) artificial intelligence (AI) professionals claiming that KM is a domain specific to AI and the associated development of expert systems, (b) information technology (IT) professionals claiming that KM is a domain specific to IT through the implementation of technologies that capture and codify knowledge, and (c) human resource management (HRM) professionals claiming that KM is a domain specific to HRM through programs that build organizational culture (Swan & Scarbough, p. 12).

Kenney (2000) supplemented the previous examples by describing how consultants, research institutions, and commercial organizations located within Silicon Valley disseminate knowledge. He explained that knowledge tends to flow more easily between networks of practice than different types of communities of practice located within the same organization. In this case, successful KM must recognize that competitive processes and different agendas, activities, and priorities may inhibit the acceptance of KM (Swan, 2003). These examples suggest that the way communities of practice define and apply KM can create barriers to the dissemination and further adoption of KM as a discipline for the transfer or diffusion of knowledge.

Barclay and Pinelli (1997) advocated that successful KM should utilize strategies and technologies from multiple disciplines that best meet the needs of the community or network of practice. They emphasized that a systematic approach for blending the theories and practices of domains such as library and information science, organizational science, and computer science be used "to examine the nature of knowledge-based work and model, elucidate, and manage both explicit and tacit knowledge resources" (Barclay & Pinelli, p. 907). These strategies will help to reduce barriers to the adoption of KM across varying communities and networks of practice.

Existing Boundaries

Initiatives in KM often conflict with existing boundaries established for the creation and diffusion of new knowledge as well as boundaries designed to discourage knowledge sharing (O'Dell & Grayson, 1998). Successful KM initiatives must consider existing structural and relational processes that help define existing boundaries within networks or communities of practice. Wiig (2000a) advised that KM activities be established and integrated with preexisting and ongoing efforts related to knowledge sharing. KM processes that ignore the existing "organizational personality" (O'Dell & Grayson, p. 17) of a network or community often conflict with established standards and cultural values. Without existing boundaries, communities or organizations lose their perspective or sense-making ability to recognize what knowledge exists and why it is needed (Boland & Yoo, 2003). In these situations, the applications of KM processes often create, rather than reduce, barriers to knowledge diffusion.

Economic Constraints

Economic costs are also a potential barrier to KM. Networks or communities of practice require leadership and the commitment of resources for KM to be successful. Murray noted that KM related resources require "codification of knowledge …, education, and sometimes changing an organization to value knowledge sharing. All these take time, money, and senior management attention" (2000, p. 184). Salient to these issues are the difficulties in valuing the return on investment for resources allocated to KM. Strassmann (1999) has written of the economic and accounting difficulties associated with valuing KM within organizations. The challenges of establishing KM as an asset and valuing knowledge as intellectual capital have acted as barriers to the adoption of KM by many organizations and communities (Davenport & Prusak, 2000).

The task of motivating stakeholders to participate within environments established by KM may also require resources such as time and money. The difficulties associated with valuing KM and intellectual capital have also created challenges in the determination of incentives as a form of motivation for participating within knowledge-based activities. Stevens (2000) has suggested that KM initiatives that lack incentives will experience low levels of collaboration by stakeholders. Debate exists over the best strategy for motivating participants to collaborate within a network or community of practice. Potential incentives have included free educational programs, awards, and additional income (Krogh, Ichijo, & Nonaka, 2000; Stevens). Krogh, Ichijo, and Nonaka also described that in addition to challenges in determining effective motivational rewards, it is also very difficult to measure “knowledge performance” (p. 253) or the ability of stakeholders to create and share knowledge. Regardless of the measurements or motivations used, KM will be less likely to succeed if initiatives do not demonstrate benefit to the stakeholder for participation and collaboration within the network or community.

Technocentric Solutions

Krogh, Ichijo, and Nonaka (2000) noted that KM related processes often fail when knowledge, especially tacit knowledge, is equal to information. Many of the existing methodologies used in KM rely on vendor (supply-side) derived software that controls knowledge in the same way as information (Stewart, 2002). According to

Stewart, a common characteristic of these tools is to feature structural or technological solutions that ignore the need for relational or cognitive processes. These processes assume that all knowledge is valuable, and the task of KM is merely to record or capture existing knowledge (McElroy, 2003). Technocentric solutions ignore the need for socialization and collaboration necessary for the transfer and diffusion of existing and new knowledge. Remez (2003a) advised that successful cases of KM characteristically place 80% emphasis on individuals and culture, with the remaining 20% dedicated to technology.

Stewart (2001) explained that technologies used to replace face-to-face interaction or socialization decrease the transfer of tacit knowledge and reduces the potential for reflection and knowledge creation. KM related technologies that treat knowledge as information usually fail to detect the spontaneous and self-evolving nature of knowledge (Krogh, Ichijo, & Nonaka, 2000; McElroy, 2003). Therefore, KM strategies based strictly on technology and supporting infrastructure are effective at transferring explicit knowledge and limited in ability to capture and transfer tacit knowledge. These technocentric KM solutions also fail to sustain the necessary production of new knowledge leading to innovation (McElroy).

Despite the barriers associated with technocentric solutions, information technologies are essential for supporting collaboration between large organizations or global communities of practice. KM related technologies must match strategic objectives related to (a) the collection, storage, transfer, and use of context; (b) sustaining collaboration; and (c) enabling communication. Measuring the value returned from KM technologies is often difficult. However, expectations of these technologies should never exceed the objective of exchanging knowledge between individuals (Remez & Desenberg, 2003).

Over-reliance on knowledge management tools.

A second barrier to KM identified by Krogh, Ichijo, and Nonaka (2000) is the over-reliance on building KM related tools. Suppliers in anticipation of knowledge-based needs by communities or networks of practice develop supply-side KM tools. Information policies that adopt and enforce the utilization of these tools often fail since their utility rarely supports the processes and creation of knowledge that self-evolve within various communities. Krogh, Ichijo, and Nonaka and Stewart (2002) recommended that the stakeholders within a community should determine the features and utilities offered by KM tools. These tools should sustain the ability to evolve with the needs of the community. Community members often reject tools that are predetermined in their structure and utility (Stewart, 2002). KM related tools support, "trust, care, and personal networks" among the stakeholders of a community or network of practice (Krogh, Ichijo, & Nonaka, p. 2). Tools that do not support these characteristics may deter from the successful implementation of KM within networks or communities of practice.

Leadership Requirements

Regardless of the strategy or purpose of KM, networks and communities of practice must have leadership and participation from their stakeholders (Wenger, 2000). Davenport and Prusak have portrayed KM as "part of everyone's job" within a community or network of practice (2000, p. 107). However, KM leadership is responsible for developing strategies for establishing knowledge-sharing cultures, advocating communities of practice, and applying KM related “tools and technology, education, taxonomy, and resources” (Bennet & Neilson, 2003, p. 526). While some evidence supports the self-evolving characteristic of knowledge-based environments (McElroy, 2003; Wheatley, 1999), it is widely acknowledged that stakeholders lose a sense of purpose and reduce their participation within knowledge-based environments that lack organization, articulated objectives, and leadership (Davenport & Prusak; Krogh, Ichijo, & Nonaka, 2000; Wenger, 2000).

Stakeholders that can serve as “knowledge activist[s]” should administer leadership within knowledge-based organizations (Krogh, Ichijo, & Nonaka, 2000, p. 147). Krogh, Ichijo, and Nonaka suggested the concept of a “knowledge activist” as individuals, working groups, or organizations that serve to provide leadership in the creation and diffusion of knowledge (p. 147). Knowledge activists serve as the coordinators of knowledge creating activities within and among various environments. In describing the role of the knowledge activist, Krogh, Ichijo, and Nonaka made the following observations.

> They will have to build up trust by demonstrating staying power and a desire for continuous collaboration. They will have to master the delicate art of attentive inquiry and dialogue, through which they can proceed to attach the intent of each community to the knowledge vision. It almost goes without saying that they have to act with integrity, at times proposing changes to the vision if it seems too ambitious, unclear, or in conflict with ongoing knowledge-creation initiatives. (p. 159)

Krogh, Ichijo, and Nonaka used the term “microcommunities of knowledge” as a way to describe the spontaneous diffusion of knowledge that cross formal boundaries (2000, p. 153). Microcommunities may reside within network and communities of practice. Relational communications and socialization are the primary means for transferring knowledge within communities. Microcommunities are often comprised of working groups that specialize in transferring tacit knowledge and building concepts or prototype processes for knowledge sharing. Leaders must consider the nature of microcommunities and not use KM as a means to control their ability to transfer and diffuse knowledge. Krogh, Ichijo, and Nonaka warned that to do otherwise risks rejection of KM by the network or community of practice.

Privacy and Security

Remez described the most obvious barrier to KM as "the concerns of citizens with privacy and security" (2003b, p. 217). Knowledge management systems and processes must consider ways to manage risks from threats such as natural disasters, terrorism, cyber terrorism, e-crime, and other acts that may disclose confidential information. Information technology, security, and legal experts should ensure protection of data and information contained within knowledge management systems and environments. Processes for protecting data and information must also consider the impact of freedom of information and privacy legislation on the ability to manage knowledge environments (Jamieson & Handzic, 2003). A breech of security or confidentiality within a knowledge-based environment will diminish trust and adversely affect the ability of KM as a process for knowledge diffusion and transfer.

GAIN, Knowledge Management, and Government Information Policies – A Recommendation for the Identification and Evaluation of Information Policy Related to Issues in Public Disclosure

Knowledge management is a relatively new concept in the information sciences (Maier, Hädrich, & Peinl, 2006). Literature normally illustrates KM in terms of potential economic or commercial benefit (Davenport & Prusak, 2000; Maier, Hädrich, & Peinl, 2006). Considerations and processes foreshadowing the advent of KM have included terminology such as “information or Internet economies” (Hundt, p. 2000) and “knowledge-based companies” (Alvarez, 1998, p. 103). Effects of government information policies on the flow and access of information are documented (Brown, 1989; Hernon, McClure, & Relyea, 1996; Hundt, 2000; Sinclair, 2006). However, existing research does not address the relationships between government information policies and KM that attempt to control public disclosure of information collected and shared on a global scale.

GAIN represents a KM related initiative that is not specifically concerned with stimulating the economic condition of a single company or culture. The true value of GAIN will be as a network that will facilitate the diffusion of existing and new knowledge beneficial to all society. The degree to which GAIN will provide economic advantages to participating airlines and related businesses remains unknown. The information and knowledge shared within the GAIN system may eventually prove to be a competitive advantage for those companies that participate. However, the potential of GAIN as a social asset that might save lives is paramount to commercial or economic advantages. For this reason, GAIN will most likely develop strong ties to local and national government information policies.

GAIN is a U.S. government initiative in knowledge diffusion. The U.S. government has an extensive history supporting the flow of information. Historically, the U.S. government has provided information policies supporting various models of knowledge diffusion. For example, U.S. government information policies have long supported the diffusion of U.S. scientific and technical information (Pinelli, Barclay, & Kennedy, 1996) and the creation of globally networked information networks and communities of practice (McClure & Ryan, 1996).

The challenges facing governments in formulating GAIN related information policies are similar to those issues faced by the U.S. government's development of information infrastructure during the 1800s and 1900s. Creating non-threatening policies that foster an environment of trust (Davenport & Prusak, 2000) will be of prime concern to the GAIN initiative. Bridging cultural differences with policies that enhance trust has been and will most likely remain a prime issue for debate within the GAIN conferences and related working groups.

Participating within the GAIN system will demand the ability to meet various standards and related network infrastructure. Socio-economic differences will most likely require government action to provide subsidies as well as policies to assure equal and timely participant access to the network. A major challenge for both local and international governments will be to consider ways to "equalize" the competitive differences that may be influenced by the knowledge shared among the GAIN participants. Governments may have to consider ways to transfer skills, analytical techniques, and required equipment to all participating airlines in the GAIN program.

GAIN participants have expressed deep concern over the ramifications of liability associated with the risks inherent to public disclosure and sharing airline safety information and knowledge. The GAIN concept will have little chance for success without adequate policies that address privacy, security, and the misuse of information or knowledge. Knowledge is tacit or explicit and often traceable to its original source. Individuals considering the contribution of safety information or knowledge to the GAIN database will likely not participate if they perceive substantial risk in exposing themselves to civil, legal, or company retribution. A major challenge to governments will be to develop policies and agreements that enforce uniform legislative standards that protect contributors to the GAIN system from liability or personal harm.

Improving the diffusion of new and existing knowledge occurs through information policy interventions and program interventions (McElroy, 2003). Burger has described information policy as the “human attempt to solve information control problems” (1993, p. 65). GAIN is a program initiative requiring the evaluation of related government information policies. Various global constituents are currently proposing and debating government information policies related to the facilitation of GAIN. Evaluations of proposed information policy may be cursory or in depth, and analyzed from within a framework of scientific, social, or political knowledge (Burger). Burger suggested that a potentially promising effort is to create a framework for evaluating proposed information policy in a new area where the potential for creating new knowledge and its distribution is unknown. The challenge is to create a framework for the evaluation for future information policy. This researcher suggests that KM can facilitate a framework for identifying and evaluating potential solutions to policy issues in public disclosure that prevent the collection and sharing of airline safety information. In this regard, GAIN is an ideal case to study the interaction between information policy and KM.

Chapter 3

Methodology

Introduction

The identification and evaluation of potential solutions to policy issues in public disclosure that prevent the collection and sharing of safety information among various organizations is a global problem within the aviation industry. The objective for this research was to develop a better understanding of how issues related to public disclosure affect the transfer and diffusion of aviation safety information and knowledge within and among various communities and networks of practice. Conclusions made in this research were based on grounded theory. Grounded theory supports the development of theoretical propositions or explanations through inductive reasoning made from the data (Mason, 2002).

An essential goal in this study was to develop a taxonomy of KM characteristics or processes central to the concept of knowledge diffusion. The primary goal was to identify and assess those KM characteristics that may serve as potential solutions to the transfer of aviation safety information or knowledge across cultural, political, and technological boundaries. Research methodology was based on theoretical constructs from information science, information policy, and knowledge management.

In the book, *Meaning and Method in Information Studies*, Cornelius (1996) suggested that the domain of information science offers a theoretical construct to study the storage, retrieval, transfer, and dissemination of information and knowledge. Borko also defined information science as a "discipline that investigates the properties and behavior of information, the forces governing the flow of information, and the means of processing information for optimum accessibility and usability" (1968, p. 3). Information science researchers also investigate issues such as knowledge diffusion, the formulation of information policies and computational analysis of document content (Hahn, 2003).

Cornelius (1996) further established information science as a field of research oriented to the study of applied settings. Within applied settings, Cornelius claimed that information science uses both qualitative and quantitative methods of inquiry. However, information and knowledge transfer studies focus on the highly complex and dynamic interaction of social processes within and across various structural, relational, and cognitive topologies. In these settings, it is doubtful that investigative methodologies based purely on quantitative measurement will provide thorough insight, or *Verstehen* (Cornelius, p. 8), to the phenomena being studied (Vickery & Vickery, 1987). Therefore, Cornelius and other authors (Patton, 2002; Vickery & Vickery) recommended interpretive or hermeneutical approaches to research inquiry where the dynamics of the environment are human-centered and under constant change.

Hermeneutical inquiry is inductive research methodology enabling understanding, or sense making (Glazier & Powell, 1992), through interpretation of data discovered in the practice or setting (Cornelius, 1996). Methodology of hermeneutical inquiry is based on constructivism and analytical philosophy. Eichelberger qualified this aspect by stating “[hermeneutists] are much clearer about the fact that they are constructing the ‘reality’ on the basis of their interpretations of data with the help of participants who provided the data to the study” (as cited in Patton, 2002, p. 115). Cornelius argued that these qualities establish interpretive methodology as viable for discovering and describing “a current, shared, intersubjective environment” (p. 25). Patton explained the following theoretical basis for conducting interpretive research,

> Hermeneutic theory argues that one can only interpret the meaning of something from some perspective, a certain standpoint, a praxis, or a situational context, whether one is reporting on one’s own findings or reporting the perspectives of people being studied (and thus reporting their standpoint or perspective). (p. 115)

Elaborating on this requirement, Cornelius (1996) provided conditions that must exist before conducting interpretive analysis. His first requirement is the need to establish a “field of objects about which we have some sense and which have some coherence” (Cornelius, p. 27). Second, the practitioner must be able to distinguish meaning between the various objects and expressions investigated. Finally, there must be human activity that recognizes the meaning and interacts with the objects in the setting studied.

Methodology for this research addressed the requirements suggested by Patton (2002) and Cornelius (1996). Taxonomy of KM was developed and interpreted for meaning related to information and knowledge diffusion. KM taxonomy of objects and related meanings provided a focus and framework to study and interpret GAIN as a case study. Data collected from various GAIN stakeholders were analyzed. Interpretations made from this data were used to identify and evaluate potential solutions to policy issues in public disclosure that prevent the collection and sharing of airline safety information.

GAIN as Subject for Case Study Research

Methodology to conduct applied research was used in this study. As a subject for applied research, GAIN is a case study demonstrating human and societal problems associated with diffusing airline safety information. Patton has defined the purpose of applied research as to "contribute knowledge that will help people to understand the nature of a problem in order to intervene, thereby allowing human beings to more effectively control their environments" (2002, p. 217). Patton added that applied research, "test[s] applications of basic theory and disciplinary knowledge to real-world problems and experiences" (p. 217). The relationship of GAIN to the domains of information policy and KM establish its validity as a case for the study of diffusion within the construct of applied research.

As a population for case study analyses, one or more organizations may serve as a "critical case" in that they are important to the phenomenon being studied (Patton, 2002, p. 236). Although not entirely a unique example, GAIN is a critical case representing government support for an independent organization seeking to diffuse information across various structural, relational, and cognitive topologies. GAIN also serves as a model for examining the collection, storage, analysis, and creation of airline safety information. Dimensions and boundaries such as time, distance, culture, public disclosure, and information policies all affect GAIN's ability to transfer airline safety information. Salient to this research are the relationships among public disclosure, information policies, and GAIN.

The study of diffusion is the "hallmark" of information policy research (Burger, 1993, p. 3). Burger defined information policies as tools used to control the access and transfer of information and knowledge. He also related the validity of examining the knowledge of a culture or entity as a means to explain the formulation of information policies (Burger). In regards to the study of information policy and knowledge diffusion, Burger stated the following,

> Whatever we believe the *raison d'etre* for information policy is or should be, or to what degree we are cognizant of our own limitations in controlling national or global information flows, we must possess some knowledge about the purported effects of carrying out a specific policy. (pp. 24-25)

Information science includes processes of descriptive or qualitative analyses for studying the dissemination of information (Cornelius, 1996). Burger (1993) used a case study approach to present evidence that information science is a valid framework from which to study information policies and knowledge diffusion. Yin (1994) recommended the interview as one of the most viable methodologies for collecting descriptive data related to case study research. Within information science, interviewing consists of developing questions, collecting data, and interpreting meaning from the data (Glazier & Powell, 1992). Interviewing as a research technique is viable for discovering and creating awareness of issues related to information and communities of practice (Wenger, McDermott, & Snyder, 2002).

Glazier and Powell (1992) also described qualitative methodologies of interviewing and text analysis as valid processes for collecting data related to case studies. Text analysis includes the statistical processing of text to derive meaning from documents (Cornelius, 1996). A relatively new form of text analysis is the linguistic processing of unstructured or naturally occurring text. Liddy (2000) referred to this process as natural language processing, or text-mining. Text-mining is "analyzing naturally occurring text for the purpose of discovering and capturing semantic information” (Liddy, para. 1). Analysis of semantic information can help discover topical structures within unstructured text. According to Liddy, text-mining is a KM tool used “to extract information for both discovery of patterns and trends as well as confirm hypotheses” (para. 4). In this study, the semantic text-mining software application *TextAnalyst* was used to help establish a taxonomy of KM and investigate relationships of KM and public disclosure to the case of GAIN.

Treatment of the Data for the First Sub-problem

The first sub-problem developed a generalized working model or “taxonomy” of KM that may be used to study global aviation or airline safety information sharing systems. Interpreting the developed taxonomy helped to establish KM related issues or methods that may potentially affect the diffusion of data, information, or knowledge within and among organizations or various communities.

Data admitted for the treatment of the first sub-problem was text documentation. The ontological position (Mason, 2002) for addressing this sub-problem was that text-based documentation related to the definition, nature, foundation, or characterization of KM is representative of KM applied in the social world. The epistemological position (Mason) for addressing this sub-problem was that the analysis and interpretation of text-based documentation can divulge a taxonomy of objects that represent evidence for aforementioned ontological properties of KM. The analysis and interpretation of text documentation used in the first sub-problem generated data required for the treatment of the second sub-problem.

Text documentation was strategically sampled (Mason, 2002) for relevance to the definition, nature, foundation, or characterization of KM. Strategic or purposive sampling has been qualified as a valid technique for "generating theory and explanation 'inductively' from or through data" (Mason, p. 125). Mason identified the following objectives of strategic sampling,

> The aim is to produce, through sampling, a relevant range of contexts or phenomena, which will enable you to make strategic and possibly cross-sectional comparisons, and hence build a well-founded argument. In this version, then, the sample is designed to encapsulate a *relevant range* in relation to a wider universe, but not to represent it directly. This might mean a range of experiences, characteristics, processes, types, categories, case, or examples and so on. (p. 124)

Text-based documents from traditional hardcopy reference material and Web-based sources served as data for the first sub-problem. Library databases and Web source material were searched for material related to the definition, nature, foundation, or characterization of KM. A review of each text document was made for face and content validity. Reliability of sampled documentation was established by using sources that have been peer-reviewed, published by recognized professional organizations, or by authors recognized within their profession.

Sampling processes for the first sub-problem were not statistically representative of the total population. Mason wrote that if "using a theoretical or purposive sampling strategy, then whether or not the sample is big enough to be statistically representative of a total population is not [the] major concern" (2002, p. 134). Purposive sampling is more concerned with selecting samples that meet a range of categories, rather than a pre-established sample size (Mason).

The investigator used semantic text-mining processes to analyze all documents accepted as samples. Semantic text-mining analysis is best suited for discovering meaning related to individual words, sentences, and documents (Schröder, 2006; Sullivan, D., 2001). D. Sullivan (p. 37) recommended text-mining as methodology for identifying taxonomies and interpreting "part-of" or "type-of" semantic informational relationships between objects identified and classified within each taxonomy. Semantic information is conceptual meaning created through interaction and interpretation of the data by the researcher (Delmater & Hancock, 2001).

Text-mining is an automated process directly related to knowledge discovery (KD) hidden in unstructured text (Jurisica, 2000; Wei, Piramuthu, & Shaw, 2003; Schröder, 2006). Jurisica characterized KD as statistical data analysis, methods in pattern recognition, and artificial intelligence applied to processes of hypothesis formulation and verification, model building, identifying outliers, information organization, and structure determination. As a method of KD, Jurisica offered the following description of text-mining software,

> Tools for text analysis are used to recognize significant vocabulary items and uncover relationships among many controlled vocabularies by creating meta-thesaurus. They can also recognize all names referring to a single entity and find multi-word terms that have a meaning of their own and abbreviations in a text with a link to their full forms. Text analysis tools automatically assign documents to preexisting categories and detect document clusters. The text analysis process can change a document from unstructured to highly structured by generating new metadata and organizing it. (Text and Web mining section, para. 1)

Text-mining includes extensive mathematical and statistical programming that requires the use of computer processing (Sullivan, D., 2001). Although text-mining software is characterized as automated, its usage does not alleviate the need for analytical or interpretative processes. Qin cautioned that when using text-mining software, the researcher needs to determine, “what data [will be fed] into the software and what kinds of patterns we expect to find, as well as decide whether or not the result is valid, novel, potentially useful and understandable” (2000, para. 4).

Additional limitations inherent to currently available text-mining software applications include (a) correctly identifying the role of noun phrases, (b) representing abstract concepts, (c) classifying synonyms, and (d) representing every topic of interest (Sullivan, D., pp. 39-42). D. Sullivan provided a list of suggestions regarding the treatment of each of the aforementioned limitations. However, the ability to address each of these limitations is subject to the functionality of individual text-mining software applications.

D. Sullivan (2001) has also described the proprietary nature of text-mining software as a concern for determining the reliability and validity of results. According to D. Sullivan, modern text-mining applications utilize proprietary syntax, terminology, and product specific tools. The variation in functionality and degrees of accuracy between currently available text-mining applications is a common problem that is not easily avoided (Sullivan, D.). Despite these limitations, authors such as Krippendorff (2004), Qin (2000), D. Sullivan (2001), Venkata (2002) and Wei, Piramuthu, and Shaw (2003) advocated the use of text-mining software applications as tools for building taxonomies and aiding in interpretive analysis for the discovery of patterns and new knowledge.

Applications of text-mining.

Data mining is a tool used for KD in databases or structured documentation. As a subset of data mining, text-mining aids in the determination of thematic and semantic relationships in and between unstructured documents (Marakas, 2002; Schröder, 2006). Text-mining applications are useful for analyzing text categorization, document clustering, and term association discovery. Text categorization assigns textual documents to one or more pre-defined categories while document clustering organizes large document collections into groups that have similar semantic relationships. Term association discovery employs search query methodology using “semantically similar and/or statistically associated terms with corresponding weights” for improving the effectiveness of information retrieval (Wei, Piramuthu, & Shaw, 2003, p. 180). These features help organizations improve capabilities for KD, knowledge creation, and decision-making (Wei, Piramuthu, & Shaw).

Text-mining applications are now widely used in industries such as financial institutions, military, security agencies, and KM consulting (Holsapple, 2003). The medical industry has adopted text-mining processes for improving the relevance and precision of information retrieval related to medical reports (Johnson, Tiara, Cardenas, & Aberle, 1997). Beckman (2003) included text-mining as a KM related tool helpful in KD within the business environment. National police and security agencies, including the U.S. Office of Homeland Security, use text-mining applications for KD and establishing patterns or key concepts that may be used to mitigate threats to national or public safety and security (Mena, 2003).

Government policy initiatives incorporate text-mining applications applied to KM initiatives and the diffusion of information. The Government of Canada qualified text-mining as a tool viable for diffusing and managing government data and information (Canada, Transport Canada, 2002). UNESCO-IHE Institute for Water Education (2003) utilizes text-mining for developing KM processes related to water management and public awareness in the Netherlands. The U.S. Chief Information Officers Council (CIOC) (2003) advocates the use of text-mining by policy makers. The CIOC advised that text-mining is useful for retrieving and correctly analyzing “enormous amounts of data that describe a problem faced by modern society” (U.S. Chief Information Officers Council, Policy Analysis section, para. 1).

The aviation industry and GAIN conducted a case study applying data and text-mining to airline safety data and information (Temin, 2004). As a proof-of-concept, GAIN and Southwest Airlines used Megaputer’s *PolyAnalyst* as a data and text-mining software tool to learn from documented safety events contained in structured and unstructured text. As applied to unstructured documentation, Megaputer’s text-mining algorithms established taxonomy and relationships that helped to understand factors contributing to airline operational safety issues (Logan & Ananyan, 2003).

Megaputer’s TextAnalyst (v2.1).

Text-mining is a new field of study based on concepts related to information retrieval, computational linguistics, natural language processing, and knowledge discovery in text (Sullivan, D., 2001). New off-the-shelf (OTS) text-mining software applications are being designed to compile, organize, and analyze “large document collections to support the delivery of targeted types of information to analysts and decision makers and to discover relationships between related facts that span wide domains of inquiry" (Sullivan, D, p. 326). This researcher used the OTS software application *TextAnalyst* (version 2.1) for proposed text-mining processes (see Appendix J).

Various authors have evaluated *TextAnalyst* for validity and reliability within a variety of settings requiring processes related to taxonomy development and knowledge discovery (Kalnine; 2000; Gupta, 1999; Sullivan, D., 2001). D. Sullivan described *TextAnalyst's* neural network approach to providing text based navigation, document and text clustering, summarization, and natural language information retrieval (p. 287). Gupta (1999) provided evidence of how these features within *TextAnalyst* have helped build a variety of case-based studies within the aviation and aerospace industries.

In terms of capability, the author compared *TextAnalyst's* functionality to other text-mining software applications, such as those produced by ClearForest, IBM, and Text Analysis International. The text-mining capability of *TextAnalyst* compared equally to other text-mining software in terms of semantic processing, development of taxonomy, and information retrieval. Many of the text-mining applications examined included features related to data mining structured text. This researcher used only unstructured text as data. *TextAnalyst* is a text-mining tool designed specifically for unstructured data (see Appendix J). Since *TextAnalyst* does not include data mining features, it is more accessible in terms of cost as compared to most other text-mining applications.

Criteria and validity for interpretations made in the first sub-problem.

In this study, text-mining helped to discover themes and relationships of KM related to issues in public disclosure that prevent the collection and sharing of data, information, or knowledge as documented in published case studies. As samples for analysis, case studies were in the form of text documents. *TextAnalyst* text-mining processes were applied to all case studies used in this sub-problem.

A project "knowledge base" (Megaputer, 2003, p. 51) containing the semantic analysis for all text documents was generated. Knowledge bases provide graphical "semantic network" of concepts discovered through text-mining (Megaputer, p. 26). A concept identified by *TextAnalyst* may be a single word or represented as a string of words. Semantic networks depict concepts, their relation to other concepts, and associated semantic weights (see Appendix J). Semantic weight for each concept discovered is defined by Megaputer "as the measure of the probability that [the] concept is contextually important" (p. 26). Semantic weights vary from 0 to 100, with 100 indicating the highest relative importance for each concept to either the parent concept or data file(s).

TextAnalyst uses a default dictionary that provides a base classification scheme for automatically analyzing natural language text files. The default dictionary may be edited as a way to improve the accuracy and relatedness of the concepts discovered through text-mining (see Appendix J). In this study, the default dictionary was edited to improve the precision and recall of concepts related to KM and issues in public disclosure that affect knowledge diffusion. The following steps were taken to edit the dictionary and validate the results for use in the second sub-problem for this study:

1. The topic “knowledge management” was added to the dictionary as a “user word” or user specified concept.[14]
2. GAIN is an entity serving as both a community of practice and network of practice attempting to disseminate best practices. Therefore, the topics “community of practice,” “network of practice,” and “best practices” were added to the dictionary as user words.
3. The topics “diffusion,” “disclosure,” “barriers,” and “policy” were added to the dictionary as user words. These concepts served as key topics from which to examine issues of disclosure and knowledge diffusion within various concepts discovered through text-mining.

Interpretations and validations made in the first sub-problem were based on a constructivist approach. Constructivism in qualitative research recognizes that new knowledge is constructed from the evidence, rather than discovered (Stake, 1995). Therefore, construct validity for interpretative methodology in this study was established using the concepts of network of practice, community of practice, and best practices as representations of reality. Network of practice, community of practice, and best practices were considered as boundaries to the interpreted KM taxonomy. Concepts under each of these categories were examined for issues related to policies, barriers, and disclosure that affect the ability of KM as a domain for managing knowledge diffusion. Using data source triangulation (Stake), identified issues were generalized across various cases in the data set and categorized into the KM taxonomy.

---

[14] User words are concepts manually added to the *TextAnalyst* dictionary and included in the semantic network regardless of relevant relationships and associated semantic weights (see Appendix J).

Data source triangulation was also conducted using a search engine within *TextAnalyst* that accepts queries stated in the form of natural text (Sullivan, D., 2001). The semantic based engine enables the search for information and relationships by semantically correlating words in the query to words in the text (see Appendix J). Scoring of the semantic correlation made from each query establishes the relational structure of sentences retrieved. D. Sullivan advised that semantic search engines based on statistical and neural-network constructs are heuristic techniques. He also warned that, "finding the correct answer is not guaranteed, but it is highly likely that you will find the answer, or something close, in many cases" (Sullivan, D., pp. 292-293). Natural text queries were used to uncover relationships between KM and knowledge diffusion. Specifically, the researcher incorporated natural language queries to help formulate greater understanding of the relationships between KM and the influences of public disclosure on knowledge diffusion.

KM taxonomy was developed by interpreting and reconciling the results from semantic analysis and natural text queries. Inductive analysis was used to delineate themes or patterns discovered within the processed data (Patton, 2002). Themes and patterns were subdivided into a classification of objects that represent a taxonomy for KM. Where possible, the researcher used information "visualization tools" such as multidimensional models, charts, or graphs to establish relationships and meaning of the interpreted KM-related taxonomy (Sullivan, D., 2001, p. 452).

Treatment of the Data for the Second Sub-problem

Issues inherent to GAIN and other similar networks affecting the diffusion of airline safety data, information, or knowledge were identified, qualified, and compared in the second sub-problem. The generalized taxonomy of KM interpreted in the first sub-problem was used as a framework to investigate these issues as related to GAIN. Methodology for this sub-problem was also used to investigate GAIN as a critical case for examining policy issues in public disclosure that act as barriers to the sharing of aviation safety information.

Data admitted for the treatment of the second sub-problem were in the form of text files transcribed from qualitative interviews. The ontological position for addressing this sub-problem was that stakeholders to the aviation industry could provide "knowledge, views, understandings, interpretations, experiences, and interactions" that are insightful to issues related to GAIN, public disclosure, and the diffusion of airline safety information (Mason, 2002, p. 63). The epistemological position for this sub-problem was that qualitative interviewing provides a meaningful and valid way to collect data related to issues of GAIN, public disclosure, and the diffusion of airline safety information. The KM taxonomy developed in the first sub-problem served as a foundation for developing questions used during each interview. A committee of three experts validated questions developed from the first sub-problem. Each expert had at least 10 years experience related to managing or researching airline safety information sharing systems. Interpretations made in the first sub-problem were combined with analysis of the interview data to develop explanations or arguments related to public disclosure and the diffusion of aviation safety information.

Qualitative interviews require the investigator to, “talk interactively with people, to ask them questions, to listen to them, to gain access to their accounts and articulations, or analyze their use of language and construction of discourse” (Mason, 2002, p. 64). Therefore, strategies for designing the interviews in this study included “standardized open-ended” and “informal conversational” techniques for interviewing (Patton, 2002, p. 349).

Standardized open-ended interviews require the construction of questions prior to the interview (Patton, 2002). Standardized questions were developed from key issues, insights, and interpretations made in the treatment of the first sub-problem. Patton characterized standardized open-ended questions as a method for reducing interviewer effects. Standardized open-ended questions also offer a structure of qualitative data easily evaluated or compared. However, standardized open-ended interviews may constrain the respondents’ ability to relate unique circumstances. Therefore, processes associated with informal conversational interviewing were also used in this study. While not as systematic as standardized questioning, informal conversational interviewing was used to collect data specifically related to the respondent and their relevant circumstances. Patton recommended the combination of these two methodologies in that, “the interviewer remains free to build a conversation within a particular subject area, to word questions spontaneously, and to establish a conversational style but with the focus on a particular subject that has been predetermined” (p. 343).

A stratified purposeful sampling design (Patton, 2002) was used to select subjects for interview data collection. GAIN stakeholders were strategically selected using the following categories: (a) members of GAIN’s community of practice, (b) members of other previous and existing aviation safety sharing information systems, (c) pilots, and (d) government aviation authorities. Many other potential sampling categories of stakeholders to the global aviation industry exist. However, the aforementioned groups are the most predominant types of stakeholders currently involved with addressing issues of public disclosure and the sharing of aviation safety information.

Mason (2002) warned of the difficulty associated with predetermining sample sizes within qualitative research. The actual sample size used in qualitative research often "emerges" as the research is being conducted (Patton, 2002, p. 246). In qualitative methodologies, the final established sample size is often a function of "what it is you need to compare, and the extent to which the sample you have generated will enable you to do that" (Mason, p. 134). Therefore, an initial pool of three subjects was identified in each of the stratified sampling categories. From this initial pool of subjects, a strategy of "chain sampling" (Patton, p. 242) was followed throughout the research process. Chain sampling identifies, "cases of interest from sampling people who know people who know … what cases are information rich" relative to the study and problem being solved (Patton, p. 243). The sampling strategy for this sub-problem emphasized depth and not breadth of sample size and quality. A goal of the interview process was to collect data that is information rich as related to issues of public disclosure and the diffusion of aviation safety information.

Content analysis was conducted on the data collected from interviews. Content analysis refers to "any qualitative data reduction and sense-making effort that takes a volume of qualitative material and attempts to identify core consistencies and meanings" (Patton, 2002, p. 453). Inductive analysis and text-mining were used to find issues inherent to GAIN and other similar networks that may affect the diffusion of airline safety data, information, or knowledge. Discovered themes related to public disclosure, diffusion, and the taxonomy of KM discovered in the first sub-problem were compared and analyzed with data collected in the second sub-problem.

A goal for this sub-problem was to develop a grounded theory characterizing or explaining KM processes that potentially mitigate public disclosure as a barrier to the diffusion of aviation safety information. As a form of analysis, Strauss and Corbin described grounded theory as, “a set of well-developed categories (e.g., themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some relevant … phenomenon” (as cited in Patton, 2002, p. 487).

Interviewing techniques, ethics, and confidentiality.

Interviewing techniques, protocols, and analysis followed the recommendations made by Gillham (2000), Kvale (1996), and Patton (2002). It was anticipated that most interviews would be conducted using in-person meetings or the telephone. All interviews were recorded using audio tape. The investigator also made notes during each interview. An informed consent was issued to each potential interviewee. The informed consent was based on and was approved by guidelines established by the Nova Southeastern University’s Institutional Review Board (see Appendix K). The identity of all respondents were kept and will remain confidential. Data collected for the study is being kept secured for an indefinite period.

Treatment of the Data for the Third Sub-problem

Potential solutions addressing the barriers to the diffusion of aviation safety information identified in the second sub-problem need to be developed, analyzed, and presented in the third sub-problem. Once interview data is collected and analyzed in the second sub-problem, a holistic and context sensitive (Patton, 2002) approach will be made to analyze GAIN as a case study. The case study of GAIN was described and presented within a thematic framework. Themes addressing challenges and potential solutions related to information policies in public disclosure that may influence the dissemination of aviation safety information were also described.

The thematic framework was developed through descriptive analysis of the interpretations made in the first and second sub-problem. Gillham stated, "For case study research operating in the real world, quantitative data analysis has to be subjected to the scrutiny of what it might *mean* – whether or not it is statistically significant" (2000, p. 87). Correlations made in the third sub-problem were based on categorical pattern matching (Gillham) rather than statistics. A holistic analysis of GAIN was conducted based on the ontological and epistemological assumptions (Mason, 2002) established in the first two sub-problems. From these interpretations, potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information were identified and evaluated.

Issues Related to Validity and Reliability

Kirk and Miller (1987) have described challenges related to proving reliability and validity in qualitative research. The nature of interpretative or qualitative inquiry often restricts the ability of the investigator to measure reliability. A potential solution to this issue is to seek investigative processes that help to ensure “synchronic reliability” (Kirk & Miller, 1987, p. 42). Kirk and Miller described synchronic reliability as, “the similarity of observations within the same time period … [it] rarely involves identical observations, but rather observations that are consistent with respect to the particular features of interest to the observer” (p. 42).

Synchronic reliability was established by seeking data directly related to the ontological and epistemological suppositions of the study. Methods for text-mining and interviewing were standardized (Leedy and Ormrod, 2001). Additionally, specific criteria for interpreting the judgments made by the investigator were also established (Leedy and Ormrod).

Multiple approaches in methodology were appropriately selected to address each sub-problem in this proposal. Combining multiple forms of methodology increased the validity of the study and served to triangulate on more than one issue of the problem being investigated (Mason, 2002).

In addition to using multiple methodologies, this researcher also subscribed to processes that support theoretical or “construct validity” (Kirk & Miller, 1987, p. 22). According to Cronbach and Meehl, construct validity is accepted when “the theoretical paradigm rightly corresponds to observations (as cited in Kirk & Miller, p. 22). In this research, construct validity implies data corresponding to the KM taxonomy and issues of public disclosure and knowledge diffusion.

This researcher used additional means for supporting validity. These processes include the following recommendations made by Leedy and Ormrod (2001, p. 106):

1. The investigator spent extensive time (6 years) investigating and studying the research problem and related phenomena.
2. The investigator looked for cases that contradict existing suppositions, and continually revised explanations or theories until all cases related to the study were analyzed.
3. The case of GAIN and related data was described in sufficient detail so that readers can interpret their own conclusions.
4. The investigator sought expert review of the interpretations and conclusions made in the study.
5. Conclusions were provided to each respective interviewee for review and feedback.

Resource Requirements

Resource requirements for this study were minimal. The software packages *TextAnalyst 2.1*, *OmniPage Pro v12.0*, *Microsoft Word*, and *Microsoft Excel* were used in the study. Human subjects, as previously described, were required for the second sub-problem. A high quality digital voice recorder was used to record each interview. Online access to various research libraries was also used. No other facilities or resources were needed.

Chapter 4

Results

Analysis and Findings for the First Sub-problem

The first sub-problem in this study was to develop a generalized taxonomy of KM to study global aviation or airline safety information sharing systems. The subsequently interpreted taxonomy established KM related issues or methods that potentially affect the diffusion of data, information, or knowledge within and among organizations or various communities.

Data Admitted for the First Sub-problem

Data for treatment of the first sub-problem were publications sampled from the literature. Publications were purposively sampled (Mason, 2002) for relevance to the definition, nature, foundation, or characterization of KM. As further qualification of sampling validity, selected publications included descriptions or case examples of applied KM. Relevant publications were located by searching the Web using *Google*, online full text article databases such as *Ebsco*, *Infotrac*, *ScienceDirect*, and *Web of Science*, and textbooks. As recommended by Ponzi (2004), the key search phrase used was “knowledge management” in the title, abstract, or descriptor field of each record. This strategy and criteria resulted in a sample size of 134 documents (the data) for analysis in the first sub-problem.

Individual documents were the minimum unit for sampling. In relation to sampling, Popping (2000) described semantic text-mining as an analysis for mapping linguistic units across words, sentences, and paragraphs. Therefore, text-mining was performed on the entire narrative within each document rather than selections from each document’s content (Popping).

Appendix L chronologically lists and references the 134 documents used as data in the first sub-problem. Publication dates for the data ranged from 1995 to 2004. According to Ponzi (2004) and Wiig (1997), publications or other activities directly associated with documenting the characteristics or applications of KM did not appear until the mid 1990s. Therefore, published documents containing cases or descriptions of applied KM were difficult to find prior to 1995.

Sample documents used in the first sub-problem represented 117 different authors or combinations of authors. A total of 45 different publications or organizations served as source material for the data documents. The types of published documentation comprising the data and related frequencies used in this sub-problem are summarized in Table 8.

The minimum frequency of sample documents taken from any single publication source was 1 with a maximum frequency of 46 (see Table 9 and Appendix M). Examples of titles or organizations representing the most frequently used of all 45 sources in the data set are shown in Table 9. Appendix M ranks the stratified sampling and relative frequencies of all data source material used in the first sub-problem.

Table 8. Types and Frequencies of Documentation Comprising the Data Analyzed in the First Sub-problem

Documentation	Frequency
Peer reviewed journal articles	95
Chapters from published textbooks	22
Articles from professional magazines	10
Professional papers or proceedings	8

Note. See Appendix L for references to all publications serving as data in the first sub-problem.

Table 9. Most Frequently Used Sources for Data in the First Sub-problem

Title or organization	Frequency
Journal of Knowledge Management	46
Handbook on Knowledge Management	10
CIO	7
European Management Journal	4
Journal of Knowledge Management Practice	4
Knowledge Management Case Book	4
Knowledge Management: The Catalyst for Electronic Government	4
The Journal of Strategic Information Systems	4
University of Texas	4
IBM Systems Journal	3
Information & Management	3
Knowledge Management for the Information Professional	3

Note. Titles or organizations shown represent the top 25% of data sources used in the analysis. See Appendix M for all 45 publishing titles or organizations and frequencies as source material for the data in the first sub-problem.

Data Processing in the First Sub-problem

Documents used as data in this sub-problem were collected as Microsoft Word (.doc) files, HTML files, PDF files, and paper copies. Paper copies were scanned using the OTS optical character recognition (OCR) software application *OmniPage Pro v12.0*. Scanned paper files were converted and saved as .doc files. PDF documents were also converted into .doc files using *OmniPage Pro*. HTML documents were saved in Microsoft Word as .doc files.

Content proofing was applied to data documents converted to .doc files. The following steps were taken to proof each .doc data file.

1. All documents were examined for correct spelling. American English was used as the standard to examine variations in English spelling (e.g., “centre” changed to “center”). Other languages were not edited.
2. Grammar was not edited. The investigator of this study believed that changing original grammar would potentially bias the semantic qualities of the data.
3. Reference sections to each document were deleted. It was determined that the inclusion of references indigenous to each document biased the results of text-mining. *TextAnalyst* processed references as complete sentences and assigned semantic weights to each reference. This inclusion biased the semantic importance of content within each document.[15]
4. Errors created through the OCR scanning process were corrected. These corrections included the removal of duplicate words, editing or removal of

[15] Specific examples include semantic weights assigned to city locations and names of publishing companies listed in references. TextAnalyst also translated titles of publications and articles as sentences and assigned semantic weights.

unidentified characters, and adjusting irregular spacing between words within sentences.

Data analyzed using *TextAnalyst* must be in the form of plain text files (.txt). Therefore, all edited .doc files were saved as individual .txt files. Since *TextAnalyst* establishes statistical weights of words within a sentence structure (Megaputer, 2003), .txt files were examined to make certain sentence structure was not damaged during file conversion.[16]

Tables, graphs, and various images original to the published documentation were lost during the conversion to .txt files. The removal of this material had minimal impact on the validity of the analyses made in the sub-problem for the following reasons. First, the meaning and content of most of the lost elements were described within the text of each published document. This information was preserved during file conversions. Secondly, most of the textual content depicted in the tables, graphs, or imagery were not in a sentence structure. Consequently, most of the text in tables, graphs, and images lost through file conversion would not have been accurately processed within *TextAnalyst*.

On completion of final proofing for sentence structure, all data files were imported into *TextAnalyst* for semantic processing. Semantic processing of the data set was accomplished using *TextAnalyst's* default settings and default dictionary.

---

[16] Sentence structure was often affected when saving .doc files as .txt files. The conversion would occasionally cause paragraph breaks to be inserted within various sentences. For accurate semantic processing, *TextAnalyst* also requires a period at the conclusion of a sentence.

Semantic processing using TextAnalyst's Default Dictionary.

Semantic processing was applied to all data files using *TextAnalyst's* default dictionary.[17] All combined data files processed consisted of 28,274 sentences. The maximum number of sentences per .txt data file was 1,630 and the minimum was 23 sentences. Sentence frequency was positively skewed across the data set with an average of 209 sentences and a median of 191 sentences per .txt data file. The file containing 1,630 sentences was created from the publication *Strategic Intentions: Managing Knowledge Networks for Sustainable Development* (Creech & Willard, 2001). In terms of sentence frequency, this file was determined an outlier to the data set. A Kolmogorov-Smirnov test showed frequencies of sentences to be distributed normally with removal of this document.[18] However, Creech and Willard's publication is an extensive case example describing global knowledge networks. Therefore, the document was retained as data in the study.

TextAnalyst identified 5,252 nodes using the default dictionary. Nodes are semantically important words or word combinations that are assigned semantic weights and paired or "linked" with other elements (Megaputer, 2003). Nodes are displayed with paired semantic weights (W_1, W_2), indicating the concept's semantic importance to its parent concept W_1, and semantic importance to all semantic concepts in the data set W_2. For example, semantic analysis of all .txt data files identified the concepts "knowledge management" and "system" as a node pair. Knowledge management was ranked as a parent concept with system as a semantically linked subordinate concept. A semantic weight of $W_2 = 99$ was calculated and assigned to knowledge management by

[17] See Appendix J for information describing the use and validity of the default dictionary.
[18] Kolmogorov-Smirnov distribution (K-S) = 0.059, ($P > 0.20$, $a = 0.050$).

TextAnalyst. In this example, “system” had a semantic weight (W_2) of 99 in relation to the entire data set. However, the subordinate semantic relationship of system to knowledge management was assigned a weight (W_1) of 52.

Nodes are the basic unit of analysis in the first sub-problem. Therefore, the reliability of *TextAnalyst’s* stability in identifying nodes and their semantic weights were examined. Popping (2000) recommended testing the reliability of text-mining software by comparing the results of multiple analyses using the same dictionary, software settings, and data set. *TextAnalyst’s* semantic processing was applied twice to all data documents using the default dictionary and identical software settings. The results of both analyses were saved and compared. Node identification and semantic relationships were exact in both analyses.[19]

Establishing validity and reliability of content analysis and semantic relationships.

In discussing sampling validity related to content analysis, Andrén stated, “The realism of a certain set of data consists of its connection with some significant problem or with the purpose of the study, i.e., its relevancy” (1981, p. 51). Fattori, Pedrazzi, and Turra (2003) addressed the challenge of determining validity of content analysis generated using text-mining software. They recommended that the process of validation rely on the analyst’s understanding of the text-mining tool and knowledge of the subject matter contained in the data. This strategy for validating the data to the concept of knowledge management was used in the first sub-problem and is described in the

[19] The same test for reliability was also conducted on a smaller subset of .txt data files. Node identification and related semantic weights in this test were identical.

abovementioned admissibility of the data. Fattori, Pedrazzi, and Turra also recommended this criterion for determining the validity of semantic relationships of nodes derived from text-mining analysis.

Semantic validity "ascertains the extent to which the categories of an analysis of texts correspond to the meanings these texts have within the *chosen context* [italics added]" (Krippendorff, 2004, p. 319). Fattori, Pedrazzi, and Turra (2003) identified reading each document, using statistical comparisons, and visualizing through graphical tools as methodology suitable for validating semantic relations in taxonomy development. These techniques are used in this sub-problem and in subsequent sections of this study.

Validity and reliability of the data set to the concept of "knowledge management."

TextAnalyst's semantic processing using the default dictionary produced 662 nodes related to knowledge management as a semantic concept. All concepts (W_1) linked to knowledge management are documented in Appendix N. Concepts in Appendix N have linked semantic weights of 2 or greater.[20]

In addition to reading and interpreting each document for relevance to the domain of KM, the degree of "correspondence and connection" (Popping, 2000, p. 140) of the data to the concept of knowledge management was also measured. Correspondence is the degree of realism to some facts or truths represented by the data. Connection is the degree of realism represented by the data to a specific problem or purpose. Popping described

---

[20] Default settings for *TextAnalyst's* semantic network analysis display concepts with a semantic weight of 3 or greater and linked concepts with a semantic weight of 2 or greater. See Appendix J for a description of *TextAnalyst's* semantic network.

the difficulties of measuring these relationships and stated, “Validity studies in text analysis are hardly performed” (p. 143).[21] Krippendorff (2004) also agreed that studies designed to analyze semantic validity are atypical. He explained the interpretative nature of assigning meaning to chosen context used in text analysis as a key barrier to assessing validity.

Popping (2000) and Krippendorff (2004) suggested correlative analysis as a method potentially viable for measuring semantic validity. Specifically, they recommended correlative analysis of semantic weights from one test as compared to criterion data generated from another test. In this sub-problem, the semantic weights of the concept, knowledge management and corresponding nodes, were compared to semantic weights derived from an alternate data set using *TextAnalyst*. The alternate data set was comprised of the definitions of knowledge management presented in Appendix A. Textual definitions in Appendix A were processed in an identical manner to the data analyzed in this sub-problem using the default dictionary.

TextAnalyst located a total of 69 nodes from the 63 sentences comprising the definitions of KM data set taken from Appendix A. The analysis found 34 nodes (W_1) semantically linked to knowledge management in the definitions of KM data set. These concepts were compared to exact concepts linked to knowledge management in the data set. Some nodes mutual to both data sets were interpreted as common terms (see Appendix J) and not included in the comparison. After removal of these nodes, 16 concepts were determined valid to knowledge management in the definitions of KM data

[21] Saris-Gallhofer, Saris, and Morton (1978) provided an example of measuring correspondence and connectedness in a study measuring the semantic differential of taxonomies generated through manual interpretive processes. Fattori, Pedrazzi, and Turra (2003) measured variations of correspondence and connectedness within and among documents automatically clustered using PackMOLE text-mining software.

set. Table 10 lists the concepts used in the comparison along with their semantic weight linked to knowledge management.

Table 10. Concepts with Semantic Weights (W_1) Linked to KM in the Study's Data Set and the Definitions of KM Data Set

Nodes	Study data (W_1)	Definitions of KM data (W_1)
Knowledge	100	100
Management	100	100
Technology	43	71
Information	46	66
Organization	62	62
Business	47	45
Intellectual	17	45
Activity	33	29
Enterprise	17	29
Intellectual Capital	12	29
Strategy	41	29
Creation	20	17
Discovery	(0, missing)	17
Executive	17	17
Performance	24	17
Understanding	18	17

Note. A correlation R statistic of .91 was determined after regressing W_1 values of concepts in the study data set with W_1 values of the same concepts in the definitions of KM data set (see Appendix A).

According to Krippendorff (2004), correlative validity in context analysis measures the extent one data set may be representative of another data set. Krippendorff provided evidence of linear correlation as a method for determining the strength of this representation. He recommended that confidence values of .80 or higher indicate reliable relationships in context analysis. In this regard, a linear correlation was conducted using the data sets described in Table 10.

With the exception of the concept "discovery," all nodes found in the definitions of KM data set were semantically related to knowledge management in the study's data set. A correlation (R = .91) of semantic weights (W_2) existed between both data sets. This correlation was interpreted as evidence that the context of the data used in this study was directly related to knowledge management. Based on correlative evidence and the aforementioned sampling strategy, the data set was accepted as valid for use in the first sub-problem.

Developing the Taxonomy of Knowledge Management

A hermeneutical interpretation was used to develop the taxonomy of KM. Krippendorff (2004) provided the following description of hermeneutical analysis related to computer generated text-mining,

> I call computer aids in this research tradition interactive-hermeneutic – *interactive* because the categories of analysis and choices of analytical constructs are not fixed, and content analysis categories become apparent to the analysts in the process of reading if not actively interrogating their texts; and *hermeneutic* because the process of analysis is directed by the analysts' growing understanding of the body of texts. (p. 303)

Krippendorff (2004) added that interactive-hermeneutic interpretation is iterative and continues until a level of satisfactory understanding is accomplished. Understanding occurs when review of the texts mirrors the analysts' background. Krippendorff qualified understanding derived from hermeneutic-interpretation as "always a temporary state, and the analytical results of this approach to content analysis are always thought to be incomplete" (p. 303).

Developing and validating the custom dictionary.

Neuendorf (2002) warned not to rely on text-mining results generated solely from default dictionaries. Default dictionaries usually contain basic vocabularies not related to problem solving in specific domains. Therefore, developing a customized dictionary was the first step toward building the taxonomy of KM.

Development of the customized dictionary followed the procedures recommended by Krippendorff (2004), Neuendorf (2002), and Popping (2000). Krippendorff offered the following ontological foundation for customized dictionaries applied to text-mining,

> The simplest theory of meaning, and the one that dominates coding/dictionary approaches, derives from taxonomy, the idea that texts can be represented on different levels of abstraction, that there are core meanings and insignificant variations of these cores, or that important meanings are thinly distributed in a body of text and need to be identified and extracted. (p. 283)

Meaning in the customized dictionary was developed and derived through thematic concept mapping. In text-mining, thematic concept mapping is the process of developing and assigning meaning (themes) to nodes representing an expansive group of concepts or semantic relationships. Nodes established as themes are interpreted as both subjects and concepts (Popping, 2000).

Thematic text-mining is an iterative process beginning with an *a prior* coding scheme applied to dictionary development. Popping (2000) described *a prior* coding schemes as an interpretive process beginning with concepts taken from theory, practice, or the research problem(s). In this analysis, themes were identified and validated from (a) theoretical constructs related to the research problems, (b) concepts grounded in practice and documented in the literature, and (c) other concepts found semantically valid through text-mining and interpreted as related to the nature of the study.

Dependent words or synonyms were assigned to user specified words (themes) defined in the custom dictionary. Instances of dependent words are automatically replaced by the related user specified word or theme during text-mining processing (see Appendix J). All themes and dependent words were validated for face validity by examining each term in the data as a key word in context (KWIC). Krippendorff (2004) described KWIC and face validity in content analysis as relying on reading text to determine the plausibility or degree of acceptance for each theme or dependent word. According to Krippendorff, using KWIC to determine face validity is based on common sense, challenging to measure, and often highly reliable when interpretations are made within frameworks of shared values.

Thematic concepts used in the custom dictionary.

Thematic concepts used in the custom dictionary were identified or interpreted from the study's research problems, the literature, and from text-mining analysis. The research problem in this study was to identify and evaluate potential solutions to policy issues in public disclosure that prevent the collection and sharing of safety information among various organizations. The first sub-problem was to develop a taxonomy of knowledge management and generalize that taxonomy to barriers that may affect knowledge diffusion. From these statements, the following themes were identified and added as user words to the custom dictionary (see Appendix J).[22]

1. *Knowledge management:* The theme knowledge management was identified from the first sub-problem. Text-mining the data using the default dictionary determined the semantic weight for knowledge management as $W_2 = 99$. Knowledge management was not linked subordinate to any other concept. The theme knowledge management is parent to all other nodes in this study.
2. *Knowledge:* The theme knowledge was identified from the first sub-problem. Text-mining using the default dictionary determined the semantic weights for knowledge as $W_1 = 100$ in relation to knowledge management and $W_2 = 99$ in relation to all nodes in the data set.
3. *Organization:* The theme organization was identified from the problem statement. Organization had semantic weights of $W_1 = 62$ in relation to knowledge management and $W_2 = 100$ to the data set using the default dictionary.
4. *Policy:* The theme policy was identified from the problem statement. Policy had semantic weights of $W_1 = 8$ in relation to knowledge management and $W_2 = 99$ to the data set using the default dictionary.
5. *Disclosure:* The theme disclosure was identified from the problem statement. As a concept, disclosure was not semantically related to knowledge management. Disclosure had a semantic weight of $W_2 = 38$ in relation to the data set using the default dictionary.

[22] Text-mining the data set using the custom dictionary produced a total of 4,647 nodes.

6. *Diffusion:* The theme diffusion was identified from the problem and sub-problem statements. Diffusion had semantic weights of $W_1 = 2$ in relation to knowledge management and $W_2 = 99$ to the data set using the default dictionary.

In addition to the above themes, interpretive analysis developed concepts grounded in practice and documented in this study's review of the literature. Of importance were themes related to GAIN as a community and network of practice.

1. *Community of practice:* The theme, community of practice, was interpreted from literature characterizing GAIN as a community of practice. Community of practice was not semantically related to knowledge management (W_1) or all nodes in the data set (W_2).
2. *Network of practice:* The theme, network of practice, was interpreted from literature establishing GAIN as a network of practice. Network of practice was not semantically related to knowledge management (W_1) or all nodes in the data set (W_2).

Additional themes identified through text-mining and interpreted as relevant to the study were also added as user words to the customized dictionary. These concepts were selected by considering their relationship to the study's problem statement and examining each node's semantic weight (W_1) in relation to the theme of knowledge management.

1. *System:* The theme "system" was interpreted from text-mining the data using the default dictionary. System was interpreted relative to issues important to this

study – such as information sharing systems and systems of networks and communities of practice. System had semantic weights of W_1 = 52 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.

2. *Technology:* The theme “technology” was interpreted from text-mining the data using the default dictionary. Technology was interpreted relative to issues important to this study – such as information, network, and computing technologies. Technology had semantic weights of W_1 = 43 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.
3. *Learning:* The theme “learning” was interpreted from text-mining the data using the default dictionary. Learning was interpreted relative to issues important to this study – such as learning environments, awareness, and sharing best practices. Learning had semantic weights of W_1 = 37 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.
4. *Culture:* The theme “culture” was derived from text-mining the data using the default dictionary. Culture was interpreted relative to issues important to this study – such as punitive cultures or organizational cultures. Culture had semantic weights of W_1 = 29 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.
5. *Individual:* The theme “individual” was interpreted from text-mining the data using the default dictionary. Individual was interpreted relative to issues important to this study – such as an individual practitioner, employee, manager, or stakeholder. Individual had semantic weights of W_1 = 24 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.

6. *Performance:* The theme "performance" was derived from text-mining the data using the default dictionary. Performance was interpreted relative to issues important to this study – such as knowledge performance, organizational or individual performance, and airline safety performance. Performance had semantic weights of W_1 = 23 in relation to knowledge management and W_2 = 99 to the data set using the default dictionary.

Figure 1 summarizes the above themes and their semantic weights (W_1) related to knowledge management using the default dictionary. Each theme was added as user words to a custom dictionary in *TextAnalyst*. In the following section, user words categorized as dependent, common, and deleted were added to the custom dictionary (see Appendix J).

Dependent, common, and deleted words used in the custom dictionary.

Developing a custom dictionary requires repeated text-mining processing as user words are interpreted or identified, categorized, and added to the dictionary (Popping, 2000). In this study, text-mining processing was repeated and results examined to interpret vocabulary and develop user words hermeneutically. Dependent words were identified or interpreted and assigned to themes saved in the custom dictionary. Dependent words are words considered synonymous to themes or other user words. Popping recommended identifying dependent words by using examples on hand

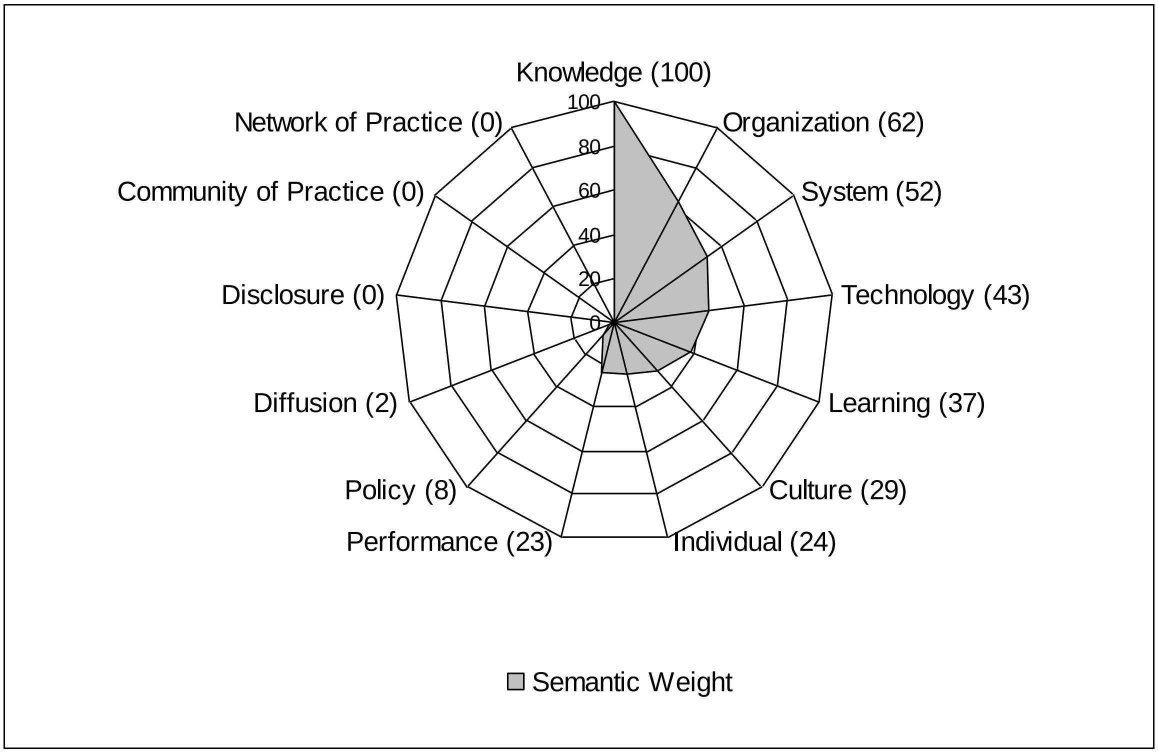

Figure 1. Themes and semantic weights (W_1) in relation to knowledge management – default dictionary.

or examining all data text for potentially related synonyms. Known examples, such as "KM" as dependent to the theme of knowledge management and the plural "organizations" as dependent to the theme of organization, were set as dependent words in the custom dictionary. Concepts interpreted as synonymous to the nature or meaning of themes were added as dependent words. Examples of these interpretations include the concept "conversation" as dependent to the theme diffusion and "philosophy" as dependent to the theme policy.

Themes were examined in the data as KWIC to discover or interpret other dependent words. Examples of these discoveries included the concept "communities of interest" as dependent to the theme communities of practice and the concept "knowledge-based systems" or "KBS" as dependent to the theme system.

Synonyms for themes and interpreted dependent words were identified using *Roget's New Millennium™ Thesaurus*. All synonyms were examined for occurrence as KWIC. Synonyms or interpreted concepts not found as a KWIC in the data were not included as dependent words in the custom dictionary. Appendix O lists the aforementioned themes (see Figure 1) and their associated dependent words used in the custom dictionary.

Developing the customized dictionary included interpretations made to identify semantically ranked concepts set as "common" or "deleted" words (see Appendix J). Adding common or deleted user words increases the accuracy of text-mining results by *TextAnalyst* (Megaputer, 2003).

Indicating a common word (or concept) in the custom dictionary modifies text-mining processing. Common words are not ranked semantically significant unless they occur in relation to an established theme. Examples of common words added to the customized dictionary include, "action," "senior," and "world." Appendix P lists all common words added to the custom dictionary.

TextAnalyst excludes deleted concepts from semantic processing, regardless of semantic importance. Examples of deleted words added to the custom dictionary include "based," "many," and "year." Appendix P lists all deleted words added to the custom dictionary.

Concepts with W_1 values less than 4 were not analyzed as dependent, common, or deleted terminology. Nodes beneath this threshold were interpreted as redundant, irrelevant, or insignificant to this analysis.

Text-mining using the custom dictionary.

Text-mining was applied to the data using the custom dictionary. With the exception of the theme “knowledge,” W_1 values increased for all other themes interpreted using the default dictionary. Knowledge had the highest W_1 using the default dictionary. Therefore, “knowledge” decreased in semantic importance relative to increases in other thematic W_1 values using the custom dictionary. These increases suggest that the custom dictionary was useful in identifying and extracting additional meaning related to each theme (Popping, 2000). Figure 2 depicts each theme with related W_1 values generated from text-mining using the custom dictionary. A comparison of W_1 values for each theme using the default and custom dictionaries is shown in Figure 3.

A goal of this research was to develop a KM taxonomy focused on policy issues related to public disclosure that may affect knowledge diffusion. Therefore, the aforementioned themes (see Figure 2) were analyzed in relation to the concepts of knowledge management, diffusion, disclosure, and policy. For example, content representing the semantic relationships of culture to knowledge management, diffusion, disclosure, and policy were individually analyzed. This pattern of analysis was repeated for each theme.

To increase accuracy and precision of retrieved concepts, semantic summarization (see Appendix J) was applied to content representing the relationships between nodes.

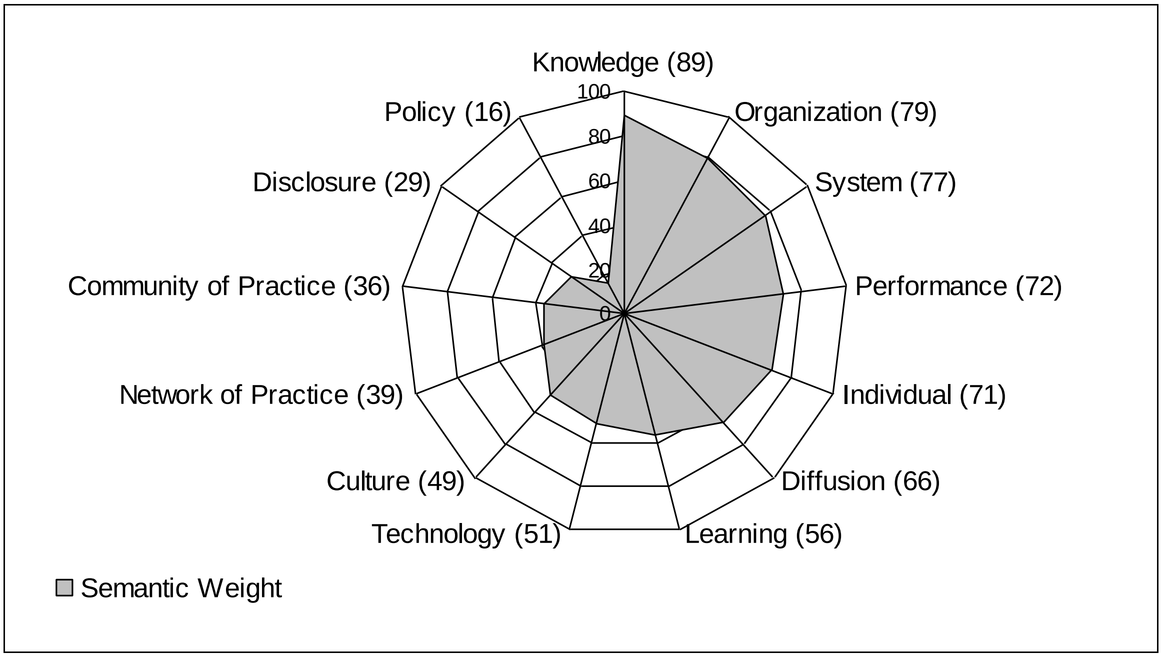

Figure 2. Themes and semantic weights (W_1) in relation to knowledge management – custom dictionary.

Content derived from summarization represented semantic levels of $W_2 \geq 90$. Levels of $W_2 < 90$ often produced content redundant to concepts retrieved within the $W_2 \geq 90$ summarization. However, in some cases summarized content for a thematically linked relationship was very limited or similar to content summarized in other relationships. For these situations, the precision of the analysis was decreased by incrementally lowering the semantic weight threshold to $W_2 \geq 50$ and subsequently to $W_2 \geq 1$, if required. The content was reexamined at each threshold level for the possibility of concepts unique to the specific semantic relationship investigated.

Ontologies relating KM, diffusion, policy, and public disclosure were interpreted from each theme's semantic summary. Ontological interpretations elucidate and add meaning to themes within an abstract model of the phenomena being studied

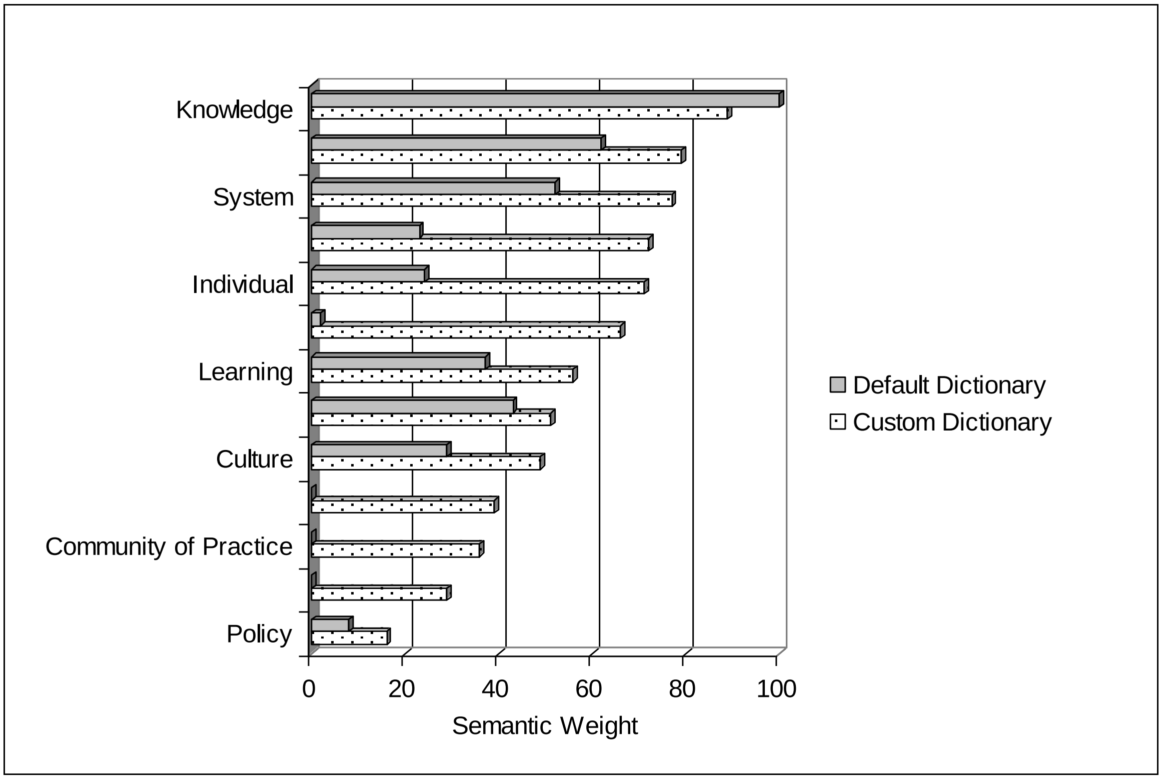

Figure 3. Comparison of themes and semantic weights (W_1) in relation to knowledge management – default and custom dictionaries.

(Doherty, Lau, Kaur, & Jain, 2005; Leroy & Chen, 2005). Ontologies were interpreted and assigned as subordinate to each related thematic relationship in the taxonomy. The following sections describe the interpretations and subsequent formulation of the taxonomy and related ontology for the first sub-problem.

Taxonomy and Related Ontologies of Knowledge Management

Knowledge and knowledge management.

Knowledge had a semantic weight of W_1 = 89 in relation to knowledge management. Content representing semantically linked themes of knowledge and knowledge management consisted of 3,770 sentences. Case examples in the content described the relationship of KM to knowledge as a system of processes used to align needs and applications of knowledge with various goals and visions of an organization (O'Dell et al., 2003). O'Dell et al. documented a company adopting and developing KM as an essential component to organizational planning and business modeling. They also described the importance for determining budget requirements needed to support KM initiatives.

Semantic analysis revealed many important concepts describing the purpose for managing knowledge or wisdom. Hariharan (2002) derived categories of knowledge from a study of businesses entitled the *ABC Group KM Case Study*. In this study, Hariharan recognized KM as the act of identifying sources of tacit and explicit knowledge. KM then diffuses these types of knowledge as best practices. Diffusion is accomplished by managing people, technologies, and communities such that knowledge is leveraged across a variety of boundaries (Hariharan).

Smith and McKeen (2003b) presented another semantically significant description describing relationships of KM to knowledge. In this work, a forum of KM practitioners examined multiple cases of applied KM. They established a consensus for KM as a concern of managing people, processes, and tools as applied to promoting, encouraging, and facilitating knowledge sharing.

A case study presented by Davenport and Völpel (2001) described KM as an attention management activity. They related how companies such as Hewlett-Packard and Chrysler assign managers the duty of paying attention to the identification, valuation, and application of knowledge. In these settings, KM is a strategy for managing knowledge as a resource.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “knowledge” and “knowledge management.”

1. Determine management responsible for adoption, development, and continuous implementation of KM.
2. Identify needs and potential applications for knowledge (tacit and explicit).
3. Align needs and potential applications for knowledge with visions and goals of an organization.
4. Identify sources of needed knowledge.
5. Determine people, processes, and tools for managing knowledge diffusion.
6. Determine budgetary requirements to support KM initiatives.
7. Determine methods for evaluating knowledge diffusion.

Knowledge and diffusion.

Diffusion had a semantic weight of $W_1 = 71$ in relation to knowledge. Content representing the semantically linked themes of knowledge and diffusion consisted of 4,160 sentences. Relationships of knowledge to diffusion were characterized in case examples as various processes or demands to share information or knowledge. For example, Fang, Hong, Bock, and Kim (2002) explained that Japanese and Korean organizations seek ways to improve the sharing of knowledge. They observed that organizations seek to progress knowledge diffusion by enhancing social processes and infrastructures supporting knowledge sharing. Correspondingly, Mason and Pauleen (2003) described the perceptions and practices of knowledge sharing by various New

Zealand companies. These companies advocated identifying and reducing barriers to social and physical mechanisms designed for sharing of knowledge.

Mason and Pauleen (2003), O'Dell et al. (2003), and many other authors emphasized the importance of identifying boundaries to knowledge sharing as a role of KM. For example, Mason and Pauleen identified in various business cases the lack of leadership and trust and fear of sharing a competitive advantage as just a few of the potential barriers to knowledge diffusion. Murty (2003) described how KM teams within various industries identified potential barriers to knowledge diffusion. The teams developed inventories of potential barriers, along with practices that facilitate the flow of knowledge. Some of the barriers identified included selectively sharing knowledge to manipulate power and hoarding knowledge. Processes identified for improving knowledge diffusion included holding KM workshops and brainstorming sessions (Murty).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "knowledge and diffusion."

1. Identify known and potential ways to enhance knowledge diffusion (social and infrastructure).
2. Identify known and potential barriers to knowledge diffusion (social and infrastructure).
3. Identify known and potential solutions to barriers of knowledge diffusion (social and infrastructure).

Knowledge and disclosure.

Disclosure had a semantic weight of $W_1 = 33$ in relation to knowledge. Content representing semantically linked themes of knowledge and disclosure consisted of 737 sentences. Managing access and security of information and knowledge (explicit and tacit) were semantically significant themes interpreted from the content. Examples of these concepts included work by McConnachie (1997), listing KM processes used by the Dow Chemical Company for managing intellectual property. In this case, Dow was concerned with protecting ownership of intellectual property and trade secrets. Dow's management established licensing agreements to control access to intellectual property. They also appointed management dedicated to evaluating and implementing ways to secure intellectual property and trade secrets. Dow viewed these processes as strategies to help sustain competitive viability and company performance (McConnachie).

Some organizations were more concerned with providing global access to knowledge than protecting against disclosure. In one case, the World Bank implemented processes facilitating global access to information and best practices for mitigating poverty (Denning, 2003). In order to enhance access across international boundaries, the World Bank created awareness and training programs for nations interested in accessing information and expert advice at the bank.

Identifying and abiding national laws or legislative acts related to privacy or disclosure were also semantically important concepts. Lasky and Tare (2002) provided examples of Australian privacy laws that vary by state governments. They recommended KM as the discipline within government and private organizations responsible for identifying and following applicable privacy laws.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "knowledge and disclosure."

1. Identify known and potential ways (social and infrastructure) for enhancing access to information and knowledge (explicit and tacit).
2. Identify known and potential ways (social and infrastructure) for securing access to information and knowledge (explicit and tacit).
3. Identify applicable regulations or laws affecting access or security of information and knowledge (explicit and tacit).

Knowledge and policy.

Policy had a semantic weight of $W_1 = 13$ in relation to knowledge. Content representing the semantically linked themes of knowledge and policy consisted of 207 sentences. Policy was semantically significant to concepts of disclosure and KM decision making as applied to sharing knowledge. Policy is described in some cases as philosophy for strategic decision-making applied to the development and application of knowledge (Smith & McKeen, 2003b). For example, Lloyd (1996) described a case where knowledge managers debated policies that would balance structured knowledge sharing systems with informal processes used to disseminate knowledge. In this case, policies advocating casual or relaxed communication processes would likely enhance creativity while potentially reducing strategic efficiencies in the company. Examples of these concerns included risk of transferring knowledge critical to competitive advantage and costs associated with re-engineering business practices that reflect adoption of KM practices (Lloyd).

Many cases endorsed leadership or management efforts establishing knowledge or KM policies as essential to successful knowledge transfer. Denning (2003) described how the World Bank established a board responsible for developing KM related policies for the organization. The bank's KM board established organizational polices requiring all units to adopt formalized processes for considering and managing knowledge. In another example, Wiig (2000b) analyzed policies used by civil servants to enhance knowledge sharing. In this study, government leadership published KM policies such as creating respect for each individual's interest, creating environments of trust, and providing motivation to learn.

Concerns of policy transcend all areas of KM. In addition to factors related to disclosure, policy addresses issues such as information or knowledge sharing standards (Lasky & Tare, 2002), targeting recipients of knowledge transfer (Creech & Willard, 2001), and developing incentive or motivational strategies for knowledge sharing (Gibbert & Krause, 2002).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "knowledge and disclosure."

1. Establish leadership or management for developing KM related policies.
2. Define and formalize visible policies for developing and implementing KM processes and infrastructure.

Organization and knowledge management.

Organization had a semantic weight of $W_1 = 79$ in relation to knowledge management. Content representing semantically linked themes of organization and knowledge management consisted of 2,418 sentences. The theme organization was identified in context with managing organizational structures (e.g. businesses or communities of practice) and the identification and structuring of knowledge. In a case presented by Roth (2003), KM is responsible for identifying and organizing knowledge domains, such as experts or communities of practice. KM also identifies and structures the relationships among these organizations in ways that facilitate knowledge transfer (Roth).

KM is accountable for organizing information and knowledge in ways that enhance knowledge transfer. Hariharan (2002) documented a series of cases demonstrating the importance of KM as a management activity for creating and structuring inventories of knowledge. These organizational structures of knowledge are made visible and accessible within and among strategic partners to the entity or communities of practice (Hariharan).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "organization and knowledge management."

1. Inventory, structure, and make visible sources of knowledge within and among organizations.
2. Establish strategies for organizing knowledge domains within and among organizations.

Organization and diffusion.

Diffusion had a semantic weight of $W_1 = 69$ in relation to organization. Content representing semantically linked themes of organization and diffusion consisted of 2,333 sentences. Much of the content from this analysis was redundant to concepts discovered in the above ontology of organization and knowledge management. In that analysis, organizational processes were also semantically linked to diffusion. However, semantic summarization in this analysis divulged concepts qualifying the importance of establishing and coordinating KM leadership across all organizations. Examples of organizational leadership advocating ways to share best practices for managing KM within and among organizations were cited in many of the cases (Abou-Zeid, 2002; Beveren, 2003; Hariharan, 2002). In these cases, leadership coordinating and implementing KM best practices within and among organizations was considered essential to knowledge diffusion.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "organization and diffusion."

1. Establish leadership for the implementation and coordination of KM within and among various organizations.
2. Establish methods (social and infrastructure) for the diffusion of KM best practices within and among various organizations.

Organization and disclosure.

Disclosure had a semantic weight of $W_1 = 32$ in relation to organization. Content representing semantically linked themes of organization and disclosure consisted of 425 sentences. Cases in the data described mapping the flow of knowledge within and among organizations as essential to controlling access or disclosure. For example, Wiig (1997) described the importance of mapping or modeling the flow of organizational knowledge using a variety of KM software tools. Gupta (2001) presented case examples in the global financial industry highlighting the importance of mapping knowledge flows among organizations that compete, collaborate, and are located in varying geographic regions. In these cases, mapping the flow of knowledge among the organizations helped to identify existing and necessary levels of access to knowledge.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “organization and disclosure.”

1. Establish and implement processes and tools for mapping the flow of knowledge within and among organizations.
2. Identify existing and required boundaries to the flow of knowledge within and among organizations.

Organization and policy.

Policy had a semantic weight of $W_1 = 17$ in relation to organization. Content representing semantically linked themes of organization and policy consisted of 170 sentences. Concepts discovered in this analysis highlighted the importance of establishing strategic policies advocating the generation and application of knowledge within and among organizations (Lloyd, 1996). Lloyd's investigation determined that the lack of established and shared knowledge management policies often deters knowledge diffusion within multi-national organizations.

In cases describing challenges to implementing global knowledge networks, Graham and Pizzo (1996) identified the need to establish methods for communicating KM policies and related management philosophies to all members of collaborating organizations. Although related to cultural concerns, these considerations are fundamental to building support of KM policies by all stakeholders to participating organizations (Lloyd, 1996).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "organization and policy."

1. Establish and share KM policies within and across all participating organizations.
2. Develop methods (social and infrastructure) for the diffusion of KM policies and philosophies within and across all participating organizations.

System and knowledge management.

System had a semantic weight of $W_1 = 77$ in relation to knowledge management. Content representing semantically linked themes of system and knowledge management consisted of 2,195 sentences. Concepts in the data describe knowledge management as a domain for managing systems of people, processes, and tools applied to various knowledge strategies and settings (Gottschalk & Khandelwal, 2003; Platt, 2000; Smith & McKeen, 2003b). In a case analysis of the 3M Corporation, Brand (1998) described KM systems as integrated structures of people and technologies enabling knowledge transfer within all areas of the corporation.

The data offered many examples of KM systems. Platt (2000) described the use of Java-based software systems used to store and disseminate information in law firms. Knowledge workers in government agencies use expert decision support systems to help solve their own problems (Salisbury, 2003). In other examples provided by Murty (2003), managers refer to mentoring and collaboration teams as KM human resource systems used to improve knowledge sharing.

Text-mining also divulged an extensive content describing system as a strategy for implementing knowledge management. In this context, many authors described cases demonstrating systematic approaches to implementing KM (DeTore & Balliet-Milholland, 2003; Moffett, McAdam, & Parkinson, 2003; Wiig, 2000b). The most significant application of this concept was described as using a systems approach to mapping knowledge flows and aligning KM systems that could be used to manage those flows (Chase, 1997a; Macintosh, Filby, & Kingston, 1999; Murty, 2003).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “system and knowledge management.”

1. Systematically identify and align integrated structures of people and technologies that may be used to manage knowledge flows.

System and diffusion.

Diffusion had a semantic weight of $W_1 = 70$ in relation to system. Content representing semantically linked themes of system and diffusion consisted of 1,961 sentences. As in the previous section describing system and knowledge management, this analysis produced many examples of KM systems used to enhance knowledge diffusion. Additional examples of these systems included integrated software programs for online learning (Na Ubon & Kimble, 2002), global networks supporting knowledge-based forums (Pan & Leidner, 2003), and systems of communities of practice serving as strategic alliances (Creech & Willard, 2001).

Cases provided evidence that knowledge diffusion is enhanced through dedicated management of social and technological subsystems within entities or cultures (Chase, 1997a; Pan & Leidner, 2003). Along with dedicated management, stakeholders to KM systems should be provided with proper training and, if necessary, facilities or equipment needed to access the systems (Creech & Willard, 2001; Rubenstein-Montano, Buchwalter, & Liebowitz, 2001). The challenges associated with these requirements are reduced and knowledge diffusion is enhanced if KM systems are relevant to the needs of the setting, simple in design, and practical in use (Levett & Guenov, 2000).

Knowledge diffusion is accelerated in environments where KM systems are integrated and their use becomes routine to the work environment. O'Dell et al. (2003) described a case where the daily use of portals provide just-in-time information and enhance collaboration. Successful KM systems, such as those used at the World Bank, must be technologically supported and integrated with other relevant information systems (Denning, 2003).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "system and diffusion."

1. Provide dedicated management and support to KM systems.
2. Provide proper training and infrastructure needed to access KM systems.
3. Develop or select relevant and easy to use KM systems.
4. Integrate relevant KM systems with each other and the work environment.

System and disclosure.

Disclosure had a semantic weight of $W_1 = 34$ in relation to system. Content representing semantically linked themes of system and disclosure consisted of 399 sentences. Semantically significant content described KM systems as methods or tools for providing access to explicit and tacit knowledge (Gottschalk & Khandelwal, 2003; Platt, 2000). Pan and Scarbrough (1998) described how successful KM systems in knowledge-based organizations provide rapid and easy access to explicit and tacit knowledge. In designing and implementing these types of efficient KM systems, protecting the privacy of stakeholders is paramount (Schrimer, 2003).

Schrimer (2003) identified privacy as fundamental to building stakeholder trust in any KM system. Companies, such as IBM and Lotus, have developed access control software and privacy issues committees to address concerns of disclosure in their customer KM systems. Schrimer also advised that successful KM systems reveal relationships among data sources and entities without diminishing trust. Not identifying these relationships reduces knowledge transfer and diminishes the ability to gain greater meaning from KM systems. Therefore, KM systems must be flexible in allowing various levels of protection against disclosure (Schrimer).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "system and disclosure."

1. Develop or select KM systems that enable protection against unwanted disclosure of stakeholder information and information revealing the relationships among stakeholders.

System and policy.

Policy had a semantic weight of $W_1 = 21$ in relation to system. Content representing semantically linked themes of system and policy consisted of 190 sentences. Text-mining in this analysis produced few concepts relating system and policy to the epistemology of KM.[23] Content did produce evidence that entities should adopt policies and procedures for the systematic integration and use of KM systems (Herder, Veeneman, Buitenhuis, & Schaller, 2003; Schrimer, 2003; Wiig, 2000b). In this context, policies and procedures were primarily related to usage of and access to KM systems.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "system and policy."

1. Develop policies and procedures for the systematic integration, use, and control of KM systems.

---

[23] Content in this analysis revealed many relationships of policy and system to other concepts not directly related to the epistemology of KM (e.g., policy related to global banking systems or to systematic processes for business development).

Performance and knowledge management.

Performance had a semantic weight of W_1 = 72 in relation to knowledge management. Content representing semantically linked themes of performance and knowledge management consisted of 1,807 sentences. Many cases in the data described KM as a means to improving the efficiency and effectiveness of performance within organizations (Bennet & Porter, 2003; Ladd & Ward, 2002; Murty, 2003). KM in relation to performance was often qualified as a means to improve quality through sharing of best practices and faster learning (Bennet & Porter; Davenport & Völpel, 2001; Murty, 2003). Chase (1997a) also described how global organizations use KM processes to improve performance by reducing management and operational errors.

This analysis also revealed cases demonstrating ways to improve KM systems and motivate stakeholders to support and participate in these systems. Examples for improving performance of KM systems included sharing development costs and risks by all stakeholders to the system and developing networks of practice (Lasky & Tare, 2002; Franz, Freudenthaler, Kameny, & Schoen, 2002). Establishing pay and non-pay incentives for motivating stakeholder participation or facilitation in knowledge sharing programs was also a significant concept in the data (Lasky & Tare, 2002; Gibbert, Jenzowsky, Jonczyk, Thiel, & Völpel, 2002).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “performance and knowledge management.”

1. Align KM processes to support specific organizational and individual performance goals.

2. Identify and implement incentives to improve stakeholder facilitation or participation within KM initiatives.

Performance and diffusion.

Diffusion had a semantic weight of $W_1 = 71$ in relation to performance. Content representing semantically linked themes of performance and diffusion consisted of 1,901 sentences. Cases in this analysis showed the importance of measuring or benchmarking increased value or performance resulting from efforts related to KM (McConnachie, 1997; van der Spek, Hofer-Alfeisa, & Kingma, 2003). These situations also demonstrated that knowledge diffusion increased when KM was directly linked to improved innovation, creating intellectual capital, or improving the efficacy of organizational processes (Freeman, 1999; Roth, 2003).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "performance and diffusion."

1. Establish methods for measuring or demonstrating the impact of knowledge diffusion on issues related to performance.

Performance and disclosure.

Disclosure had a semantic weight of $W_1 = 32$ in relation to performance. Content representing semantically linked themes of performance and disclosure consisted of 332 sentences. Concepts in this analysis relating performance and disclosure were interpreted as redundant to the aforementioned concepts relating knowledge and disclosure. Cases emphasized control of access to intellectual capital as a factor influencing the efficacy of the organization. Privacy safeguards were shown to affect the effectiveness of information sharing systems in supporting the needs of the user (Schrimer, 2003). In this regard, controlling the ability to identify and access intellectual capital influenced the quality and productivity of performance by knowledge workers (Ryske & Sebastian, 2000).

Summarization in this analysis did not produce concepts interpreted as providing new meaning to the taxonomy. Therefore, no ontology was added to the taxonomy from this analysis.

Performance and policy.

Policy had a semantic weight of $W_1 = 20$ in relation to performance. Content representing semantically linked themes of performance and policy consisted of 168 sentences. Content in this analysis provided case examples advocating KM as a tool to improve the performance of developing and implementing policy (Creech & Willard, 2001; Gabbay et al., 2003). Using KM to help develop and communicate policies was shown to improve the ability of various nations to manage processes associated with sustainable development (Creech & Willard). Gabbay et al. described how various communities of practice use networks to improve awareness of KM policies within and among organizations.

Summarization in this analysis did not produce concepts interpreted as providing new meaning to the taxonomy. Therefore, no ontology was added to the taxonomy from this analysis.

Individual and knowledge management.

Individual had a semantic weight of $W_1 = 71$ in relation to knowledge management. Content representing semantically linked themes of individual and knowledge management consisted of 1,777 sentences. Many of the concepts revealed in this analysis were redundant to those related to themes of learning, culture, and performance (subsequently discussed).

Cases in the data highlighted the importance of identifying individual stakeholders to KM initiatives (Gottschalk & Khandelwal, 2003; Salisbury, 2003). Specifically, organizations seek to identify individuals or other entities that may serve as a source of intelligence, expertise, or experience (Gottschalk & Khandelwal, 2003; Wiig, 2000b). Cases presented strategies for enhancing access to tacit and explicit knowledge held by individual stakeholders and organizations (Robertson, 2002).

Organizations should also seek to identify individuals that will help to facilitate or lead KM initiatives (Wiig, 2000b). In the aforementioned case by Brand (1998), experts and advocates of KM were strategically connected to other individuals. Using this strategy, transfer of tacit and explicit knowledge among individual stakeholders to the organization was increased.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “individual and knowledge management.”

1. Identify and strategically connect individuals or individual entities that may serve as a source of intelligence, expertise, or experience to the KM initiative, or serve as advocates to the KM initiative.

Individual and diffusion.

Diffusion had a semantic weight of W_1 = 74 in relation to individual. Content representing semantically linked themes of individual and diffusion consisted of 2,695 sentences. Many of the concepts revealed in this analysis were redundant to those related to themes of learning and culture (subsequently discussed). Concepts in this analysis focused on interactions and relationships of individuals to KM initiatives and infrastructure. Cases such as those presented by Herder et al. (2003) and von Krogh (2001), recommended increasing knowledge diffusion by encouraging greater participation or socialization within the KM initiative by individuals. Examples of these processes included face-to-face meetings (Joia, 2002), facilitating space and motivation encouraging informal meetings (Chase, 1997a), and hiring employees intrinsically motivated by knowledge sharing (von Krogh, 2001).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “individual and diffusion.”

1. Determine ways to increase participation of individuals within KM initiatives.

Individual and disclosure.

Disclosure had a semantic weight of W_1 = 35 in relation to individual. Content representing semantically linked themes of individual and disclosure consisted of 489 sentences. Concepts revealed in this analysis were redundant to those related to themes of diffusion and policy described throughout this sub-problem. The analysis did reveal limited content addressing concerns of individuals as related to privacy issues. Content in the case presented by Schrimer (2003) and described in the above thematic relationship of system to disclosure was also significant to individual and disclosure.

Summarization in this analysis did not produce concepts interpreted as providing new meaning to the taxonomy. Therefore, no ontology was added to the taxonomy from this analysis.

Individual and policy.

Policy had a semantic weight of W_1 = 17 in relation to individual. Content representing semantically linked themes of individual and policy consisted of 168 sentences. Many concepts revealed in this analysis were redundant to themes of policy described throughout this sub-problem. Summarization revealed limited content addressing concerns of individuals as related to privacy issues. The analysis highlighted the previously discussed concept of policy decision making as a required function of managers implementing KM (Creech & Willard, 2001). Several cases demonstrated that individuals are more inclined to support and facilitate KM policies if allowed to participate in the formulation of those policies (Creech & Willard; Lloyd, 1996).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “individual and policy.”

1. Involve individual stakeholders in the formulation of KM related policies.

Learning and knowledge management.

Learning had a semantic weight of W1 = 56 in relation to knowledge management. Content representing semantically linked themes of learning and knowledge management consisted of 922 sentences. Themes within the data focused on describing processes for learning about knowledge management (Barquin, Bennet, & Remez, 2003; Smith & McKeen, 2003b) or using KM to increase learning within organizations (Dalrymple, 2000; Platt, 2000). Platt recommended reading books and attending conferences to learn about best practices in KM. Studying case examples of learning organizations, communities, and networks of practice are also recommended as ways to learn about KM (Hariharan, 2002). Examples of processes used to increase learning within organizations included process improvement seminars, creative workshops, and online forums (Murty, 2003).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "learning and knowledge."

1. Determine and implement strategies to learn about the nature and applications of knowledge management.
2. Identify and implement known and potential KM processes that may enhance learning by stakeholders to an organization.

Learning and diffusion.

Diffusion had a semantic weight of $W_1 = 70$ in relation to learning. Content representing semantically linked themes of learning and diffusion consisted of 1,132 sentences. Cases in this analysis demonstrated that generation and diffusion of knowledge increased when opportunity and space were made available for stakeholders to learn (Ardichvili, Page, & Wentling, 2003). Fahey, Srivastava, Sharon, and Smith (2001) related mentoring, training, and development as ways to create, share, and leverage knowledge. These authors also recommended story telling and collaboration as learning processes leading to improved knowledge diffusion.

Wagner (2003) provided examples of partnering as a way for organizations to learn from each other. In these cases, transfer of knowledge was increased when partnering included learning processes strategically chosen for each collaborative initiative. Using this approach, partnering was effective for organizations desiring to share and learn knowledge regarding processes, procedures, and techniques (Brand, 1998; Wagner).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "learning and diffusion."

1. Provide time, space, and opportunity for stakeholders to participate in learning activities.
2. Determine, align, and implement learning strategies that compliment the needs of the organization and stakeholders to the organization.

Learning and disclosure.

Disclosure had a semantic weight of $W_1 = 30$ in relation to learning. Content representing semantically linked themes of learning and disclosure consisted of 186 sentences. Content in this analysis described learning as positively related to the ability to identify and access sources of information and knowledge (Contractor, & Ra, 2002; Gupta, 2001). Contractor and Ra highlighted the importance of removing barriers to sources of information as key to enhanced learning. They also caution that the removal of these barriers may lead to various risks, including loss of competitive advantage or intellectual capital (Contractor, & Ral; Gupta).

Although learning had a strong semantic relationship to disclosure, concepts interpreted from this analysis were determined redundant to the ontology for learning and diffusion. Therefore, no ontology was added to the taxonomy from this analysis.

Learning and policy.

Policy had a semantic weight of $W_1 = 14$ in relation to learning. Content representing semantically linked themes of learning and policy consisted of 67 sentences. This analysis provided limited content. Cases provided examples of entities and cultures supporting and communicating policies integrating learning as a key strategy for creating, maintaining, and leveraging intellectual capital (Gibbert & Krause, 2002; Wiig, 2000b). Various organizations advocated people development systems, team learning, and knowledge sharing as essential long term policies of KM initiatives (Ferrari & Carlos de Toledo, 2004).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "learning and policy."

1. Establish and communicate policies that sustain learning and related processes as long term KM strategies.

Technology and knowledge management.

Technology had a semantic weight of $W_1 = 51$ in relation to knowledge management. Content representing semantically linked themes of technology and knowledge management consisted of 726 sentences. Cases in this analysis provided extensive evidence that technology is a significant component of knowledge management. Proper selection and integration of KM-related technologies can improve value, quality, and utility of the knowledge management initiative (Chuang, 2004; Gottschalk & Khandelwal, 2003; Ryske & Sebastian, 2000). KM related technologies should be selected to meet the knowledge seeking goals of the stakeholder (Gottschalk & Khandelwal). Hariharan (2002), McConnachie (1997) and Wickert and Herschel (2001) provided examples of how properly selected KM related technologies improve knowledge diffusion, collaboration, work processes, and document-management within and among spatially distributed organizations.

McConnachie (1997) and Creech and Willard (2001) advocated that entities should establish management and technological support for KM technologies. Monitoring technological progress of KM technologies should be a critical role for these support groups (Takahashi & Vandenbrink, 2004). Failure to maintain or adopt new KM related technologies may diminish the ability to manage knowledge and utility of the KM initiative.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “technology and knowledge management.”

1. Identify, select, and integrate KM related technologies in relation to the knowledge seeking goals of the entity or stakeholders.
2. Establish dedicated management and technological support for KM related technologies.

Technology and diffusion.

Diffusion had a semantic weight of $W_1 = 72$ in relation to technology. Content representing semantically linked themes of technology and diffusion consisted of 722 sentences. In this analysis, Schrimer (2003) described examples of KM related technologies that continually provided stakeholders with a means to disseminate and acquire new knowledge. Schrimer, Desouza (2003), and Jermola, Lavrač, and Urbančič (2003) and many other authors described the effectiveness of using technologies such as email, group support systems, and data mining to enhance knowledge diffusion. In most of these case examples, KM technologies are not a panacea to effective knowledge dissemination. To enhance knowledge diffusion, technology should support the knowledge needs of cultural and organizational structures (Moffett, McAdam, & Parkinson, 2003). Herder, Veeneman, Buitenhuis, and Schaller (2003) emphasized that KM technology used to support social interaction will most effectively enhance diffusion. Examples of these technologies included decision support systems for team meetings and infrastructures designed to enhance the flow of knowledge within communities and networks of practice.

Summarization in this analysis emphasized the importance of selecting KM technologies that complement or support social and organizational knowledge sharing. These concepts were interpreted as redundant to the previous ontology relating technology to knowledge management. Therefore, no ontology was added to the taxonomy from this analysis.

Technology and disclosure.

Disclosure had a semantic weight of $W_1 = 37$ in relation to technology. Content representing semantically linked themes of technology and disclosure consisted of 160 sentences. Concepts in the data relating disclosure to technology were limited. Most of the content from this analysis emphasized technology as a means to enhance access, with little regard to the potential consequences of increased access.

Contractor and Ra (2002) exemplified the importance of balancing the selection of technology with the types of alliances being formed. Failure to implement technology based on the understanding of the alliance may risk undesired disclosure of individual identity as well as intellectual property. Creech and Willard (2001) and Kelly and Bauer (2003) added that KM technologies are often targeted or personalized to specific individuals. In these cases, knowledge of personal identity was required prior to the adoption of the technology.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “technology and disclosure.”

1. Evaluate the inherent risks of disclosure from KM related technologies used within and among alliances or individual stakeholders.

Technology and policy.

Policy had a semantic weight of $W_1 = 14$ in relation to technology. Content representing semantically linked themes of technology and policy consisted of 40 sentences. Very little content in the data linked concerns of policy to technology. Galliers

(1999) described a deficiency by industry to develop policies related to the integration of technology within KM systems. Cases described the need for policies that considered usability and technology standards when selecting or designing KM related technologies. Various international organizations provided examples of establishing committees for determining policies related to consistent Web interface usability and related technological standards (O'Dell et al., 2003). Other authors described the need to develop policies that control the use and access to various KM related technologies (Na Ubon & Kimble, 2002; Nielsen, in press).

Summarization in this analysis emphasized the importance of establishing policy for controlling the use and access of KM related technologies. These concepts are redundant to those found in the semantic relationships between policy and system. Determining policy for considering usability and standards related to KM technologies was interpreted as unique to this analysis. From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "technology and policy."

1. Establish policy addressing usability requirements of KM related technologies.
2. Establish policy addressing technological standards required of KM related technologies.

Culture and knowledge management.

Culture had a semantic weight of $W_1 = 49$ in relation to knowledge management. Content representing semantically linked themes of culture and knowledge management consisted of 693 sentences. In this analysis, many cases described the concept of culture as an essential consideration of knowledge management (Ardichvili, Page, & Wentling, 2003; Lasky & Tare, 2002; Na Ubon & Kimble, 2002). Establishing environments that advocate and sustain knowledge sharing as a cultural norm is considered a prime responsibility of knowledge managers (Davenport &Völpel, 2001; Hariharan, 2002).

Cases in the data provided many examples of how organizations create cultures that participate in knowledge sharing. Some organizations treat knowledge as an asset, and reward those that create and share knowledge (Currie & Kerrin, 2004; Na Ubon & Kimble, 2002). Na Ubon and Kimble also described successful knowledge sharing cultures as organizations creating environments of trust, care, and personal networks. Other examples included knowledge managers supporting the individual's need for knowledge, creating learning environments, and providing feedback to those sharing knowledge (Chuang, 2004; Mason & Pauleen, 2003, Sieloff, 1999).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "culture and knowledge management."

1. Establish strategies and processes for developing a knowledge sharing culture.

Culture and diffusion.

Diffusion had a semantic weight of $W_1 = 75$ in relation to culture. Content representing semantically linked themes of culture and diffusion consisted of 999 sentences. This analysis produced content confirming that a prime responsibility of knowledge management is to create a knowledge sharing culture (Chase, 1997a; Christensen & Bang, 2003). Establishing cultural environments of trust and shared norms or values may be the most important steps used in KM for enhancing knowledge diffusion (Gertler & Wolfe, 2004; Jermola, Lavrač, & Urbančič, 2003; Na Ubon & Kimble, 2002). Creating these types of environments is potentially more effective in supporting knowledge diffusion than implementing KM related technologies or developing formalized strategies for sharing knowledge (Currie & Kerrin, 2004; Swan & Scarbrough, 2001).

Various cases emphasized that organizations should evaluate the viability of their culture to diffuse knowledge (Currie & Kerrin, 2004; Ladd & Ward, 2002). Ladd and Ward recommended this type of evaluation as useful in determining efforts or investments that should be allocated to supporting knowledge diffusion. Efforts or resources designed to enhance diffusion may not work in cultural environments that are not trustworthy or do not support knowledge sharing values such as creating opportunity for socialization (Christensen & Bang, 2003; Ladd & Ward).

Concepts in this analysis supporting the creation of knowledge sharing cultures were redundant to the aforementioned relationships of culture and knowledge management. Evaluating the capacity of a culture to sustain knowledge diffusion was interpreted as unique to this analysis. From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “culture and diffusion.”

1. Evaluate the viability or capacity of the organization’s or society’s culture to sustain knowledge diffusion.

Culture and disclosure.

Disclosure had a semantic weight of $W_1 = 33$ in relation to culture. Content representing semantically linked themes of culture and disclosure consisted of 155 sentences. The ability to identify and socialize with individuals is shown to be the prime mode of knowledge diffusion within cultures (Bresnen, Edelman, Newell, Scarbrough, & Swan, 2003). This analysis produced concepts describing the ability to reveal relationships among individuals and entities without diminishing trust as an essential characteristic of knowledge sharing cultures (Na Ubon & Kimble, 2002; Schrimer, 2003). Ardichvili, Page, and Wentling (2003) described cases where institutional or cultural-based trust is ensured by clearly communicating how stakeholders will be protected from negative consequences of disclosure.

Protection against the potential detriments of disclosure often requires balancing security processes with requirements for socialization and other forms of access within knowledge sharing cultures. Protections against disclosure can hinder the ability of cultures to develop agreement on common purposes and processes (Desouza, 2003). This concern can be problematic in cases of globally distributed stakeholders not able to build trusting relationships through direct contact and socialization (Damm & Schindlerb, 2001).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “culture and disclosure.”

1. Determine ways to balance socialization and access within cultures with the need for protection against disclosure.

Culture and policy.

Policy had a semantic weight of $W_1 = 17$ in relation to culture. Content representing semantically linked themes of culture and policy consisted of 66 sentences. This analysis highlighted knowledge management as a process susceptible to conflict from varying cultural policies (Berdrow & Lane, in press). According to Brand (1998), cultures may vary in terms of need to control, desire for innovation, ability to provide service or leadership, and motivations to perform.

Gertler and Wolfe (2004) provided case examples of various nations attempting to develop collaborative KM related policies reflecting the needs of each culture. Pan and Leidner (2003) described a case where stakeholders developed a policy handbook for how to share knowledge within a global information transfer system. According to the authors, the handbook polices developed into cultural norms shared be all stakeholders to the knowledge sharing system.

Developing KM related polices that sustain various cultural requirements is best accomplished by carefully selecting partners to develop policy from across all participating cultures. If implemented, this recommendation will improve stakeholder trust, contribute to establishing common goals, and enhance the ability to leverage knowledge (Ladd & Ward, 2002; Wiig, 2000b).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "culture and policy."

1. Determine stakeholders from each participating culture that will contribute to formulating knowledge sharing policies.
2. Develop and implement policies for sharing knowledge across varying cultures.

Network of practice and knowledge management.

Network of practice had a semantic weight of $W_1 = 39$ in relation to knowledge management. Content representing semantically linked themes of network of practice and knowledge management consisted of 428 sentences. The phrase “network of practice” was not found in any of the documents. Approximately 12 documents made reference to the concept of knowledge networks. KWIC examinations of knowledge network identified the concept as related to aforementioned definitions of network of practice. Therefore, this analysis considers the concept of knowledge network as synonymous to network of practice.

Most references to knowledge network were in the case study *Strategic Intentions. Managing Knowledge Networks for Sustainable Development* (Creech & Willard, 2001). Approximately 58 documents used the concept of network in a variety of settings – e.g., bank networks, learning networks, communications networks, and human networks.

Knowledge networks are created by entities and societies to transfer knowledge and use the collective resources of members to create knowledge (Creech & Willard, 2001). Takahashi and Vandenbrink (2004) described businesses using peer-to-peer networks featuring shared workspaces for transferring knowledge. O’Dell et al. (2003) and Gibbert and Krause (2002) provided examples of organizations using knowledge networks to leverage global knowledge and create knowledge applied to solving specific problems.

Knowledge networks require considerable planning before implementation. Factors such as infrastructure (social and technological), costs, time, and human resources must be considered. The integration of the network with varying cultural relationships and existing networks must also be planned (Creech & Willard, 2001).

Successful knowledge networks require communication infrastructures and protocols that maintain the joint working efforts and goals of stakeholders. Shared governance supporting the visions, goals, objectives, and missions of the network must be provided. Knowledge networks require equally shared access and tools that support interaction and socialization among members (e.g., synchronous communications) (Creech & Willard, 2001).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “network of practice and knowledge management.”

1. Determine the need for and feasibility (social and technological) of implementing one or more networks of practice.
2. Establish shared governance of implemented network(s) of practice.
3. Design networks of practice such that they provide equal access to stakeholders and tools that support interaction and socialization among members.
4. Networks of practice should be aligned with the visions, goals, objectives, and missions of the network’s membership.

Network of practice and diffusion.

Diffusion had a semantic weight of $W_1 = 73$ in relation to network of practice. Content representing semantically linked themes of network of practice and diffusion consisted of 761 sentences. The concept of knowledge network was characterized as a medium and process for diffusing knowledge or innovations at local levels to those seeking knowledge or solutions at global levels (Creech & Willard, 2001; Gibbert & Krause, 2002). Creech and Willard cautioned that barriers such as trust, social relationships, personal self-interests, culture, policies, and standards may act as barriers to knowledge diffusion within and among networks.

Managers of knowledge networks can reduce or control barriers to diffusion. Cases demonstrated the need for network managers, forum specialists, and individual coaches. Network managers are responsible for maintaining the continuity and purpose of a knowledge network (Creech & Willard, 2001). According to Creech and Willard, networks often become decentralized and unfocused over time. These changes can erode the transfer of desired knowledge. They recommended establishing a network manager that regulates the ability of stakeholders to modify the structure and purpose of a network. Network managers routinely evaluate the network's effectiveness for diffusing, processing, and applying knowledge (Creech & Willard; Pan & Scarbrough, 1998).

Forum managers and coaches act as advocates assisting special interest groups or individuals in acquiring or diffusing information over the network (Chase, 1997; Pan & Scarbrough, 1998). Coaches also train stakeholders to participate in or use the network, thereby increasing the potential for knowledge diffusion (Chase).

Examples of organizations avoiding or dominating knowledge networks were presented by Peña (2002) as strategic ways to influence or control diffusion. Some organizations form networks to share non-sensitive information, thereby reducing costs through scale-of-economy. Other organizations have formed networks with strategic partners in order to block the diffusion of knowledge to key competitors (Peña).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "network of practice and diffusion."

1. Evaluate strategic rationales for establishing or participating in networks and their potential affect on knowledge diffusion.
2. Select and integrate network managers, forum specialists, and individual coaches as advocates of knowledge diffusion for the network.
3. Routinely evaluate the network's effectiveness for diffusing, processing, and applying knowledge.

Network of practice and disclosure.

Disclosure had a semantic weight of $W_1 = 31$ in relation to network of practice. Content representing semantically linked themes of network of practice and disclosure consisted of 118 sentences. Content relating disclosure to networks of practice revealed in this analysis was redundant to many of the previously described ontologies. Schrimer (2003) described cases using forums or special interests groups to evaluate privacy issues and controls throughout knowledge network systems. Examples of privacy issues and controls within networks included allowing managers to regulate the ability to identify sources and users of information and selecting software that removes metadata related to personal identity (Schrimer).

Fear of disclosure was presented as a barrier to many different types of organizations in deciding to participate within knowledge networks. Participation may expose companies to the potential loss of sensitive information or data. However, not participating in networks may diminish the competitive or creative capabilities of organizations (Peña, 2002).

Summarization in this analysis emphasized the importance of selecting processes and technologies that control disclosure in KM systems. These concepts were interpreted as redundant to previous ontologies relating knowledge management to disclosure. Therefore, no ontology was added to the taxonomy from this analysis.

Network of practice and policy.

Policy had a semantic weight of $W_1 = 24$ in relation to network of practice. Content representing semantically linked themes of network of practice and policy consisted of 84 sentences. This analysis produced limited content relating concepts in policy to networks of practice. Knowledge networks were described as KM strategy for disseminating existing policies or formulating new policies related to the objectives or goals of the participating stakeholders (Baker, Barker, Thorne, & Dutnell 1997; Creech & Willard, 2001). Most of the content in this analysis was sourced from Creech and Willard's work describing knowledge networks as a tool to develop and disseminate cultural and sustainable development policies.

Jermola, Lavrač, and Urbančič (2003) and Peña (2002) provided examples of businesses establishing guidelines for selecting participation in specific networks or network partners. These cases required network policy makers to balance the competitive nature of networks or network partners with the need for access to information or knowledge. In a related theme, Creech and Willard (2001) advised that managers of knowledge networks should evaluate KM policies of existing networks prior to forming alliances. These evaluations should consider social and technological policies related to participation as well as processes and rules for selecting or terminating involvement in a knowledge network.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “network of practice and policy.”

1. Determine social and technological policies controlling implementation and participation in a network of practice.
2. Evaluate and reconcile existing policies, goals, and objectives of individual networks of practice seeking alliances.

Community of practice and knowledge management.

Community of practice had a semantic weight of $W_1 = 36$ in relation to knowledge management. Content representing semantically linked themes of community of practice and knowledge management consisted of 381 sentences. Communities of practice are established to bring together knowledge workers and experts sharing a joint purpose or common goal (Bennet & Porter, 2003). Members to communities of practice directly interact to share views, processes, and knowledge to effect change within domains or agendas (Gabbay et al., 2003; Gloet, & Berrell, 2003). These members may actively engage in knowledge management as a way to improve performance by stakeholders around the world (Herder, Veeneman, Buitenhuis, & Schaller; 2003). Communities of practice are active in many globally distributed industries, such as oil and gas exploration (O’Dell et al., 2003), health organizations (Gabbay et al., 2003), and software development (Conway, 2003). Through direct interaction and socialization, community members build trust, values, and understanding by all participating entities or societies (Swan & Scarbrough, 2001).

Communities of practice manage standards, processes, technologies, and cultural issues required for global KM initiatives (O'Dell et al., 2003). For these reasons, the primary concerns to establishing communities of practice are the correct selection and integration of community members (Chase, 1997a; Franz, Freudenthaler, Kameny, & Schoen, 2002). Proper selection and integration of community members will lead to faster delivery of new knowledge and innovative solutions. In various cases, properly managed and staffed communities of practice improved learning and reduced operational and business mistakes made by stakeholders (Franz, Freudenthaler, Kameny, & Schoen.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "community of practice and knowledge management."

1. Establish communities of practice to manage and share knowledge associated with distributed or global problems, agendas, or goals.
2. Identify and properly select knowledge workers charged with initiating, administering, and monitoring the community of practice.

Community of practice and diffusion.

Diffusion had a semantic weight of $W_1 = 75$ in relation to community of practice. Content representing semantically linked themes of community of practice and diffusion consisted of 860 sentences. This analysis produced evidence that communities of practice effectively create and diffuse tacit knowledge related to problem solving or best practices (Fahey, Srivastava, Sharon, & Smith, 2001; Franz, Freudenthaler, Kameny, & Schoen, 2002; O'Dell et al., 2003). Communities of practice provide efficient and relevant access to expertise and intellectual capital (Franz, Freudenthaler, Kameny, & Schoen). Cases of entities using communities of practice as a strategy for knowledge diffusion include intellectual capital sharing within the automotive industry (Wolford & Kwiecien, 2003) and best practices of government transportation safety agencies (Burk, 2002).

Similar to other KM systems, factors such as trust, culture, geography, time, leadership, and funding may impede knowledge diffusion within and among communities of practice (Ardichvili, Page, & Wentling, 2003; Fahey, Srivastava, Sharon, & Smith, 2001; Franz, Freudenthaler, Kameny, & Schoen, 2002). Communities of practice that do not establish representatives serving as affiliates to other communities may experience a loss in knowledge sharing (von Krogh, 2001). Environments where varying levels of technology and standards exist also may diminish knowledge diffusion within and among communities. In these situations, sub-communities may form and further prevent the ability of the community to diffuse knowledge (Takahashi & Vandenbrink, 2004).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "community of practice and diffusion."

1. Establish formal representation and affiliation among relevant communities of practice.
2. Establish equal standards and technologies within and among communities of practice.

Community of practice and disclosure.

Disclosure had a semantic weight of $W_1 = 32$ in relation to community of practice. Content representing semantically linked themes of community of practice and disclosure consisted of 129 sentences. Cases in this analysis highlighted communities of practice as a way to encourage social interaction and face-to-face communication (Hildreth, Kimble, & Wright, 2000; Na Ubon & Kimble, 2002). Because of these characteristics, communities of practice usually create environments supporting trust and identity, thereby enhancing the transfer of knowledge (Hildreth, Kimble, & Wright). Communities of practice benefit participating stakeholders by providing identification and access to knowledge, resources, and individuals of authority (von Krogh, 2001). Berdrow and Lane (in press) provided examples of communities of practice used by international joint ventures. In these cases, communities of practice provided stakeholders to information or knowledge not widely distributed. Through established organizational and personal relationships, communities of practice also provide opportunity for learning and innovation (Berdrow & Lane; Na Ubon & Kimble).

Stakeholders use communities of practice to seek access and interaction for collaboration on activities of mutual interest (Pan & Leidner, 2003). Viability of the community of practice depends on stakeholders not misusing information or knowledge gained through collaboration. Examples of these situations include using the information or knowledge to help facilitate a personal agenda or as a way to cause harm to other stakeholders. A case study presented by Ardichvili, Page, and Wentling (2003) described examples of managing knowledge-based trust within communities of practice. In this case, KM managers used committees to verify the validity and accuracy of information distributed within the community. These managers also screened entities and individuals seeking access to the community of practice. In this process, the managers looked for evidence supporting the trustworthiness of the individual or entity in previous knowledge sharing environments (Ardichvili, Page, & Wentling).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "community of practice and disclosure."

1. Determine and implement strategies and processes for socialization and face-to-face interaction within communities of practice.
2. Determine and implement strategies and processes for managing and sustaining trust within communities of practice.

Community of practice and policy.

Policy had a semantic weight of W_1 = 14 in relation to community of practice. Content representing semantically linked themes of community of practice and policy consisted of 43 sentences. Data relating the concepts of policy to communities of practice was limited. Concepts interpreted as relevant to this analysis centered on developing policies that advocate information and knowledge as a public good owned by the community (von Krogh, 2001). This type of policy must be adopted by all stakeholders to help ensure opportunity for socialization and motivate individuals to participate within the community of practice (Pan & Leidner, 2003).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "community of practice and disclosure."

1. Determine and adopt policies advocating the dissemination of information and knowledge as a public good within communities of practice.

Table 11 summarizes the results of the taxonomy and ontology interpreted in the first sub-problem. Semantic weights and sentence frequency for each thematic pairing used in the taxonomy are summarized in Appendix U. The taxonomy and related ontology represent a generalized working model of KM. The taxonomy identifies issues that may potentially affect the diffusion of data, information, knowledge, or wisdom within and among entities or societies. This model is subsequently used in the second sub-problem as the foundation for studying issues related to information policy and disclosure that may affect the diffusion of airline safety information.

Table 11. Taxonomy and Ontology of KM

Taxonomy	Ontology
Knowledge – KM	Determine management responsible for adoption, development, and continuous implementation of KM
	Identify needs and potential applications for knowledge (tacit and explicit)
	Align needs and potential applications for knowledge with visions and goals of an organization
	Identify sources of needed knowledge

Table 11 (continued).

Taxonomy	Ontology
Knowledge – KM	Determine people, processes, and tools for managing knowledge diffusion
	Determine budgetary requirements to support KM initiatives
	Determine methods for evaluating knowledge diffusion
Knowledge – diffusion	Identify known and potential ways to enhance knowledge diffusion (social and infrastructure)
	Identify known and potential barriers to knowledge diffusion (social and infrastructure)
	Identify known and potential solutions to barriers of knowledge diffusion (social and infrastructure)
Knowledge – disclosure	Identify known and potential ways (social and infrastructure) for enhancing access to information and knowledge (explicit and tacit)
	Identify known and potential ways (social and infrastructure) for securing access to information and knowledge (explicit and tacit)
	Identify applicable regulations or laws affecting access or security of information and knowledge (explicit and tacit)
Knowledge – policy	Establish leadership or management for developing KM related policies
	Define and formalize visible policies for developing and implementing KM processes and infrastructure
Organization – KM	Inventory, structure, and make visible sources of knowledge within and among organizations
	Establish strategies for organizing knowledge domains within and among organizations

Table 11 (continued).

Taxonomy	Ontology
Organization – diffusion	Establish leadership for the implementation and coordination of KM within and among various organizations
	Establish methods (social and infrastructure) for the diffusion of KM best practices within and among various organizations
Organization – disclosure	Establish and implement processes and tools for mapping the flow of knowledge within and among organizations
	Identify existing and required boundaries to the flow of knowledge within and among organizations.
Organization – policy	Establish and share KM policies within and across all participating organizations
	Develop methods (social and infrastructure) for the diffusion of KM policies and philosophies within and across all participating organizations
System – KM	Systematically identify and align integrated structures of people and technologies that may be used to manage knowledge flows
System – diffusion	Provide dedicated management and support to KM systems
	Provide proper training and infrastructure needed to access KM systems
	Develop or select relevant and easy to use KM systems
	Integrate relevant KM systems with each other and the work environment
System – disclosure	Develop or select KM systems that enable protection against unwanted disclosure of stakeholder information and information revealing the relationships among stakeholders

Table 11 (continued).

Taxonomy	Ontology
System – policy	Develop policies and procedures for the systematic integration, use, and control of KM systems
Individual – KM	Identify and strategically connect individuals or individual entities that may serve as a source of intelligence, expertise, or experience to the KM initiative, or serve as advocates to the KM initiative
Individual – diffusion	Determine ways to increase participation of individuals within KM initiatives
Individual – disclosure	(Redundant to ontology for system and disclosure)
Individual – policy	Involve individual stakeholders in the formulation of KM related policies
Performance – KM	Align KM processes to support specific organizational and individual performance goals
	Identify and implement incentives to improve stakeholder facilitation or participation within KM initiative
Performance – diffusion	Establish methods for measuring or demonstrating the impact of knowledge diffusion on issues related to performance
Performance – disclosure	(Redundant to ontology for knowledge and disclosure)
Performance – policy	(Data did not provide relevant content sufficient for interpretation)
Learning – KM	Determine and implement strategies to learn about the nature and applications of knowledge management
	Identify and implement known and potential KM processes that may enhance learning by stakeholders to an organization

Table 11 (continued).

Taxonomy	Ontology
Learning – diffusion	Provide time, space, and opportunity for stakeholders to participate in learning activities Determine, align, and implement learning strategies that compliment the needs of the organization and stakeholders to the organization
Learning – disclosure	(Redundant to ontology for learning and diffusion)
Learning – policy	Establish and communicate policies that sustain learning and related processes as long term KM strategies
Technology - KM	Identify, select, and integrate KM related technologies in relation to the knowledge seeking goals of the entity or stakeholders Establish dedicated management and technological support for KM related technologies
Technology - diffusion	(Redundant to ontology for technology and KM)
Technology - disclosure	Evaluate the inherent risks of disclosure from KM related technologies used within and among alliances or individual stakeholders
Technology - policy	Establish policy addressing usability requirements of KM related technologies Establish policy addressing technological standards required of KM related technologies
Culture – KM	Establish strategies and processes for developing a knowledge sharing culture
Culture – diffusion	Evaluate the viability or capacity of the organization's or society's culture to sustain knowledge diffusion
Culture – disclosure	Determine ways to balance socialization and access within cultures with the need for protection against disclosure

Table 11 (continued).

Taxonomy	Ontology
Culture – policy	Determine stakeholders from each participating culture that will contribute to formulating knowledge sharing policies Develop and implement policies for sharing knowledge across varying cultures
Networks of practice – KM	Determine the need for and feasibility of implementing one or more networks of practice Establish shared governance of implemented network(s) of practice Design networks of practice such that they provide equal access to stakeholders and tools that support interaction and socialization among members Networks of practice should be aligned with the visions, goals, objectives, and missions of the network's membership
Networks of practice – diffusion	Evaluate strategic rationales for establishing or participating in networks and their potential affect on knowledge diffusion Select and integrate network managers, forum specialists, and individual coaches as advocates of knowledge diffusion for the network Routinely evaluate each network's effectiveness for diffusing and processing knowledge
Networks of practice – disclosure	(Redundant to ontology for KM and disclosure)
Networks of practice – policy	Determine social and technological policies controlling implementation and participation in a network of practice Evaluate and reconcile existing policies, goals, and objectives of individual networks of practice seeking alliances

Table 11 (continued).

Taxonomy	Ontology
Community of practice – KM	Establish communities of practice to manage and share knowledge associated with distributed or global problems, agendas, or goals
	Identify and properly select knowledge workers charged with initiating, administering, and monitoring the community of practice
Community of practice – diffusion	Establish formal representation and affiliation among relevant communities of practice
	Establish equal standards and technologies within and among communities of practice
Community of practice – disclosure	Determine and implement strategies and processes for socialization and face-to-face interaction within communities of practice
	Determine and implement strategies and processes for managing and sustaining trust within communities of practice
Community of practice – policy	Determine and adopt policies advocating the dissemination of information and knowledge as a public good within communities of practice

Analysis and Findings for the Second Sub-problem

The second sub-problem in this study was to develop a specialized taxonomy addressing issues controlling the diffusion of global airline safety information. Issues inherent to GAIN and other similar networks affecting the diffusion of airline safety data, information, or knowledge were identified, qualified, and compared to the generalized taxonomy of KM developed in the first sub-problem. These interpretative processes resulted in the development of a specialized taxonomy of KM related issues that may aid in the design and implementation of global airline safety information sharing systems.

Establishing KM Processes for Mitigation of Public Disclosure as a Barrier to the Diffusion of Aviation Safety Information

A goal for this sub-problem was to develop a grounded theory that characterizes or explains KM processes that may mitigate public disclosure as a barrier to the diffusion of aviation safety information. Methodology for this sub-problem was used to investigate GAIN as a critical case for examining policy issues in public disclosure, which serve as barriers to the sharing of aviation safety information. For these purposes, data in this sub-problem was processed and interpreted for relevance to the themes of diffusion, disclosure, and policy. Content determined relevant to these themes were further analyzed and compared to the taxonomy and ontologies of KM established in the first sub-problem.

Data Admitted for the Second Sub-problem

Data for treatment of the second sub-problem were interview transcripts obtained from stakeholders to GAIN and the global airline industry. Stratified purposeful sampling (Patton, 2002) was used to select subjects for interview data collection. Ten subjects provided interview data for this sub-problem. Stakeholders were selected strategically using the following categories: (a) members of GAIN's community of practice, (b) members of other previous and existing aviation safety information sharing systems, (c) pilots, and (d) government aviation authorities.

With the exception of government aviation authorities, interview data was collected from each stratified sampling category. Participating subjects were asked if they would recommend government representatives as potential sources of data to the study. From these recommendations, individuals affiliated with government aviation authorities in the U.S. and various European nations were invited to serve as subjects. All of these individuals declined to participate. Several government representatives indicated that participation in the study might create conflicts of interest related to their involvement with various airline safety information sharing systems. Some of these individuals stated that participation in the study might harm political and business relations between existing airlines and affiliated government agencies. Two individuals, retired from government service and no longer affiliated with airline safety information sharing systems, also declined participation.

Alternate subjects were selected in an effort to obtain data related to government aviation authorities. Two alternate subjects agreed to participate in the study. One of those subjects was an aviation lawyer with experience interacting with government representatives working with airline safety information sharing systems. The other subject was an aviation information specialist with extensive experience dealing with government aviation authorities in the Mideast and U.S. The characteristics of these and the remaining subjects that participated in this research are summarized in Table 12.

Table 12. Characteristics of Interview Subjects

Subject (S_n)	**Characteristic**
S_1	International consultant specializing in aviation safety and security information management
S_2	Mideastern aviation safety and flight information analyst
S_3	Director of a European aviation safety information sharing system and member of GAIN
S_4	U.S. airline pilot
S_5	European airline pilot
S_6	Aviation safety information specialist of a U.S. airline and member of GAIN
S_7	University professor and attorney specializing in aviation safety and aviation law
S_8	Director of a U.S. airline aviation safety information sharing system and member of GAIN
S_9	University researcher specializing in the development of aviation safety information sharing systems and member of GAIN
S_{10}	Airline pilot, past member of GAIN, and officer of an international airline pilot's association

The ontology developed in the first sub-problem was used to derive a set of standardized open-ended questions for use in each interview (see Appendix U). Three experts validated the questions for clarity and face validity relevant to the problem statement for this analysis. These questions served as a generalized framework for investigation during each interview. Not all questions in Appendix U were asked in each interview. As an aid to the interviewer, questions were categorized in relation to the themes of knowledge management, diffusion, disclosure, and policy.

Each interview began by asking the subject for information describing their background and experiences related to airline safety information sharing systems. Various questions from each category in Appendix U were asked as a way to improve understanding of the responses made by each subject. Most interviews were concluded by asking subjects for their recommendations to manage the impact of disclosure on the diffusion of airline safety information. Each interview lasted between 30 minutes and 1 hour.

Validity and reliability of the data used in the second sub-problem.

Validity and reliability of the data used in the second sub-problem was established by (a) purposefully selecting subjects qualified as stakeholders to airline safety information sharing systems, (b) soliciting from subjects information and knowledge directly related to the ontologies developed in the first sub-problem, and (c) using the customized *TextAnalyst* dictionary validated in the first sub-problem. All data content (notes and interview files) were reviewed for relevance to the taxonomy created in the first sub-problem.

Data Processing and Content Analysis in the Second Sub-problem

All interview conversations were recorded using a high quality digital recorder. Each recording was transcribed into a separate text file (.txt). Content was examined for accuracy by reading each document while listening to the corresponding audio file.

Interview subjects were also allowed the opportunity to review and "self-correct" their responses for clarity and interpretative understanding (Kvale, 1996, p. 189). Six subjects were re-interviewed to clarify comments recorded during initial interviews. All text files were examined and edited for English spelling. Grammar was not edited. Handwritten notes of salient issues were also made by the interviewer during each interview and re-interview.

Content analysis and semantic network analysis using TextAnalyst's Custom Dictionary.

Content analysis was conducted by reading each interview file. Interview data interpreted as relevant were extracted, sorted, and clustered in relation to the themes of diffusion, disclosure, and policy. Interpretive processes of indexing and pattern matching (Mason, 2002) were used to correlate extracted interview data with existing themes or to discover new themes within the KM taxonomy.

Semantic network analysis in *TextAnalyst* was used to further examine concepts of diffusion, disclosure, and policy in all interview .txt data files.[24] Text-mining was used to enhance the precision and recall of content related to these themes. The custom dictionary developed in the first sub-problem was used in *TextAnalyst* for this processing. Diffusion, disclosure, and policy were investigated in relation to the taxonomy created in the first sub-problem.

---

[24] Each interview .txt file included the remarks and questions made by each subject and the interviewer. Text-mining was conducted on a duplicate set of data files that had all interviewer content removed. It was determined that precision and recall of data (sentences provided by subjects) were more accurately associated with themes generated in the first sub-problem when interviewer content (questions) was included in the processed data files. Since *TextAnalyst* is "black-box" technology, the exact cause of this phenomena is unknown. See Appendix J for known technical information describing *TextAnalyst*.

Taxonomy and Related Ontologies Interpreted from Interview Data

Interview data was analyzed in relation to the themes of diffusion, disclosure, and policy within a thematic framework of KM. Interpretative processes focused on identifying phenomena discovered in the data that may affect the diffusion of aviation safety information.[25] This specialized taxonomy of KM related issues may aid in the design and implementation of airline safety information sharing systems.[26]

Diffusion and Aviation Safety Information Sharing Systems

Information overload.

Interview subjects described issues relating information overload as a barrier to the diffusion of aviation safety information. Subjects S_1, S_2, S_4, S_7, S_8, and S_9 indicated that extensive volumes of aviation safety information exist within most medium to large airlines. These subjects relayed how most of this information is collected independently using different processes and standards. For these reasons, information contained in many databases owned by airlines and various other organizations is difficult to analyze, and therefore difficult to disseminate (S_7).

Subject S_9 described that information overload is caused by many aviation safety information sharing processes that "ask too many questions, rather than ask the right questions." According to subject S_9, this characteristic has contributed to the development

---

[25] The author acknowledges that the discussions, taxonomy, and ontologies in this sub-problem contain issues that may be interrelated or overlap. Many of these issues have complex affects on diffusion.

[26] Subjects with experience facilitating aviation information sharing systems were asked to describe their understanding or experiences of KM. None of these subjects were aware of KM as a domain for managing knowledge diffusion or information policy. When asked about the nature or application of KM, most subjects requested clarification of the concept. One subject (S_2) suggested that, "knowledge management is probably something like GAIN is trying to do." For this reason, interpretation of interview data revealed little useful information describing or qualifying the domain of knowledge management as related to aviation safety information sharing systems.

of large quantities of collected data that are not practical to administer or diffuse. Subject S_6 indicated the need to address diffusing large volumes of data and information within an organization, prior to establishing or participating in industry-wide information sharing systems,

> The point I want to make is that before we start sharing data with others, we need to start using our own data better. Programs don't exist, or I haven't been able to find them, that allow me to use the 10,000 reports I have in a meaningful way. Why would I be interested in some other company's 20,000 reports when I can't even use my own 10,000 reports? You know, we've got to learn to walk before we can learn to run. So my interest right now is data mining my own 10,000 reports rather than sharing data. (S_6)

Subject S_8 also had similar concerns to those expressed by Subject S_6. When asked about potential benefits to global aviation safety information sharing systems, Subject S_8 offered the following response,

> I do not see a benefit to that. As I articulated before, if I am concerned about LaGuardia airspace, I'll call up colleagues at other airlines that have a lot of business, a lot of flights in and out of LaGuardia, and ask them. I really don't have the need for their data. I've got more data than I need with my own data. I don't need another airline's data to completely be lost in my data. (S_8)

In relation to quantities of collected information, subjects also described the amount of diffused aviation safety information as information overload (S_1, S_2, S_4,). As a strategy to address information overload, Subject S_4 described how most airline employees receive regular hardcopy reports summarizing various concerns related to aviation safety. According to Subject S_4, the typical employee will scan each report to identify areas of specific interests. Rarely will employees have time to read each report to learn about new concerns (S_4). Subject S_1 reinforced this concern by making the following observations regarding information overload and the dissemination of aviation safety information within their company,

> You know, we'd be overwhelmed if they gave us everything [information]. Even within our company there's too much information being released. There has to be a way to search, that narrows your field to what you want to focus on. The folks at the operational end of the sphere don't have a lot of time to sit around reading five page reports on some issue. They want the facts quickly and concisely. (S_1)

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the theme of "information overload."

1. Determine processes to manage and analyze information internal to the organization prior to participating in external information sharing systems.
2. Determine problems to be solved and types of information needed prior to collecting or sharing new information.
3. Develop effective and efficient methods to disseminate information and align these processes with the needs of stakeholders using the information.
4. Develop ways to structure and present information that will facilitate effective and efficient usage by stakeholders.

Databases and standards.

Subjects S_1 and S_3 described that most stakeholders are not aware of the variety of existing domestic or global aviation safety information databases. Furthermore, stakeholders are not usually aware of various standards used to collect, store, retrieve, and analyze aviation safety information. According to Subject S_1, most companies store aviation safety information in separate databases using different structures, taxonomies, or ontologies, and processes of analysis.

Subject S_1 indicated that aviation information sharing systems should be networked to a centralized database. Subject S_1 stated, “There is not a current database that is centralized for the sharing and dissemination of safety information, nor for lessons learned, commonalities, etc.” This interviewee believed that a centralized database containing standardized information would help to manage information overload. In this regard, Subject S_1 proposed that, “A centralized database, with standardized taxonomies, would help us manage huge amounts of information, handed out in various methods by airlines” (S_1).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of “databases and standards.”

1. Maintain and publish directories of all known aviation safety information sharing systems, networks, or databases.
2. Catalog metadata describing technologies, standards, and data relevant to each known aviation safety information sharing system, network, or database.
3. Evaluate the feasibility and benefits for developing or sharing information with centralized industry sponsored database systems.

Data mining and semantic analysis.

Subjects also described how processes for deriving interpretations or meaning of data related to aviation safety act as barriers to diffusion (S_3, S_6, S_8, S_9). Stakeholder perception often varies for definitional and semantic meanings associated with aviation safety terminology and concepts (S_6). A past member of GAIN indicated that definitional and semantic variations are significant barriers to the analysis and dissemination of aviation safety information (S_6).

Subject S_8 illustrated how variations in semantic meaning can reduce the precision and recall aviation safety data or information. In this example, Subject S_8 described how the concept of a "deviation" in flight operations may represent (a) a unique regulatory concern, (b) a pilot's assessment of flight procedure, or (c) jargon explicit to an airline. Because of this ambiguity, Subject S_8 expended considerable effort in manually reviewing retrieved reports associated with the concept of deviation. The following passages provided by Subject S_8 described this and similar challenges related to semantic interpretation of aviation safety information,

> It is difficult with all these meanings. For example, I had to find a report that announced a deviation that happened over Denver a year ago. I questioned [queried] our database of over 11,000 reports. About 200 reports came back related to coding for deviations. I started reading the reports, literally reading all the reports and codes to extract the deviation data I wanted.
>
> I may call this a "glass" and Britain will call it a "cup." So how many glasses did you break last year? Well, in Britain they broke none because they use cups. In Britain, the piece of glass that is directly in front of the captain and the first officer, they call it a CV, or a "clear view." I call it the cockpit window or the cockpit glass.
>
> For example, my aircraft encroaches on the runway 10 feet. According to the FAA that is not a runway incursion unless somebody else is coming in here to land and would have to go around. We call that type of example a runway incursion. We have 300 runway incursions; the FAA had 10 because they didn't define it a runway incursion unless someone was impacted to the point that they actually had to go around. So, again, how do you measure things and how do you define them. (S_8)

As an aid to establishing semantic interpretations, Subjects S_6, S_8, S_9, and S_{10} expressed the need for industry developed data and text-mining tools. All of these subjects indicated that these tools would be helpful in developing taxonomy. These tools should be used to supplement and enhance expert interpretation of the data, and not replace human analysis of data and development of semantic meanings (S_6).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "data mining and semantic analysis."

1. Supplement expert analysis and semantic interpretation of aviation safety information with data mining tools.
2. Select data mining applications viable to development of taxonomy and related ontology.

Taxonomy and ontology.

Subjects S_3, S_6, S_8, S_9, and S_{10} were questioned about the use of taxonomies and ontologies as a way to reduce semantic ambiguity of aviation safety information within their organizations. All of these subjects indicated that taxonomy and ontology were essential to managing and diffusing aviation safety information. Subject S_9 offered an example relating the importance of taxonomy to the interpretation of meaning and diffusion,

> Meaning gained from collected data or information comes from how you categorize that material, rather than how you analyze it. We determined that categorized data with taxonomies solicits greater information from sources – we get richer detail of information from pilots when we ask them questions about safety information according to a taxonomy. (S_9)

Subject S_6 indicated that developing a taxonomy is a continuous and iterative process. According to Subject S_6, forming a consensus toward a taxonomy is difficult since, "individuals can read those reports all day and come up with entirely different taxonomies" (S_6). In support of this observation, Subject S_9 stated, "Taxonomy is something that is always debated and refined." The following discussions by Subjects S_8, S_{10}, and S_6 also helped to explain additional challenges for developing taxonomy,

> We have a problem in putting the data in the same way every time. I might have an event that happened last year and again this year and forgot that we had that event and called it something one year and something else the next year. A lot of this is predicated on the memory of the person putting the data into the database. Luckily, we've had the same people doing this for a number of years. But, if we lose just one of our database people and when we hire a replacement, it's going to be a mess because of the different vantage points -- a new person will call things differently than the last person did. (S_8)

> One of the hardest things we had to come up with was taxonomy that provided a common event set across a whole bunch of different airlines. We were able to do it between several air carriers, which was a start. It took some real time and effort to get a few carriers to all agree on the taxonomy. (S_{10})

> We built the taxonomy for the archives based on what everybody was already using. Now we're going through it line by line, every single event type, every single threat, every single error -- trying to make sure what everybody is collecting is covered there [in the taxonomy]. We are trying to make it so that however each airline collects their data, they'll be able to figure out a way to match the data so that nobody has to change what they are already doing with their own taxonomies. (S_6)

Interpreting meaning and developing related taxonomies are even more challenging when considering the translation of reports submitted in various languages or by different cultures. Subject S_3, a director of a past European aviation safety information sharing system, made the following observations regarding these issues,

> Our system was part of an international network of reporting systems – but, it did not work! The reason for failure was cultural differences. A report written in our language was not translatable into other languages. The meaning of the report was lost! The same situation exists with reports in English translated into other languages. Our language produces a "picture" in the head of the reader. The person reading the report fills the "gaps" in the wording of the text with their own words -- this happens "all in the head." Therefore, in our language, the report is briefly written. To translate or transform the report into English, a lot more descriptions are needed. If it is done by an Englishman, the "flavor" of the content is not transferred. If a member of our culture is doing the translation, an English person will not understand the nuances in the text. It took us years to understand these "differences" and try to develop taxonomy capturing the meanings lost through translation and cultural differences. (S_3)

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "taxonomy and ontology."

1. Allocate time and expert resources for developing taxonomy and ontology.
2. Develop taxonomy and ontology as a framework for collecting and disseminating future data or information.
3. Consider the affect of cultural values on semantic meaning when reconciling or developing taxonomy and ontology.

Search strategies.

Information overload, complexities related to semantic meaning, and cultural differences also affect search behavior by stakeholders seeking aviation safety information (S_1, S_2, S_8). Subjects S_1 and S_8 explained that differences in standards and in meaning perceived as relevant to an issue cause many individuals to seek information directly from colleagues. Subjects described that most U.S. airline industry stakeholders prefer to seek information by phone calling, emailing, or talking in-person with colleagues (S_1, S_2, S_8). Personal communication was held by subjects as a way to increase trust and the ability to question validity or meaning applied to data or information (S_1, S_2, S_8).

In the U.S., industry stakeholders prefer safety conferences or symposiums as a forum for personal interaction and sharing of information (S_1). Subject S_1 explained that, "At industry conferences, individuals often feel safer sharing safety concerns, as there is usually a common feeling of everyone experiencing the same problems." One director of an airline safety information sharing system attends over 10 safety conferences per year (S_8). Subject S_8 explained the importance of face-to-face meetings and aviation safety conferences,

> I met all of my counterparts at many of the conferences. We go out to dinner. We become friends. When I have a problem that I need to handle, then I call one of my contacts and ask "what do you have in this area?" I don't want all their data. I'll just call and ask "what do you have that I could use?" I'll let my contact run the report for me. (S_8)

According to Subject S_1, many individuals in the industry also prefer forms of electronic communication such as email and online newsletters. These types of medium allow stakeholders to structure their own individual data management systems. They also enable search and retrieval processes more useful to the individual's needs (S_1). However, Subject S_8 described that processes for searching information and associated precision and recall of retrieved information as challenges related to standards, information overload, and semantic meanings,

> We do need to use word searches. For example, we had an incident where the pilots were descending from 20,000 to 15,000 feet. As they got close to 15,000, the captain raised one finger. What he meant to say was we have "1,000 feet to go." Well, we don't do that at our company. That means "flaps one." So, the co-pilot, gave him flaps one, and they were

> going very fast. They caused damage to the aircraft. I was asked to find this report, and the only way that I knew how to find it, was, I thought "one finger." I typed in the words, "one finger" in my data search, and sure enough, I got that report. You really have to find some creative ways to find reports. We have no other way to find a report like that.
>
> When you have unstructured data that's going into a database, it's difficult to extract data because you don't know what you are searching for. Let me rephrase that. You know what you are searching for, but it's difficult to get at the data, just because with unstructured data you can't see the "forest for the trees." (S_8)

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the theme of "search strategies."

1. Provide time and access for stakeholders to conduct face-to-face meetings or attend industry conferences related to aviation safety.
2. Seek or develop search tools and related strategies for individual stakeholders that will enhance retrieval of needed aviation safety information.
3. Seek or develop search tools and related information technologies enabling storage and retrieval of aviation safety information disseminated in varying formats of structured and unstructured data.

Trust, culture, and immunity.

All interview subjects believed the protection of individuals from public disclosure and retribution or punishment resulting from the sharing of aviation safety information as essential to sustaining effective aviation information sharing systems. Subject S_3 stated that, "protecting informants from punishment is the first step in creating a safety-culture." Airline pilot interviewees also emphasized the importance of assurances from employers, unions, and other stakeholders that their identity will be kept confidential (S_4, S_5, S_{10}). These pilots indicated they must be certain information voluntarily contributed will not be disseminated with any indication of their identity. All subjects indicated that successful participation of stakeholders to aviation information sharing systems is predicated on strong environments of trust, resulting from the ability to remain anonymous.

None of the participants believed that any known aviation information sharing system could completely protect the identity of participants from disclosure. Subject S_2 indicated that, “many governments have the power to access confidential data systems, if they want to.”[27] The following discussion by Subject S_7 captured similar concerns expressed by other subjects (S_2, S_3, S_4, S_5) related to disclosure,

> There are spies, there are bribes, and there are relatives in high places in any government. Even U.S. CIA operatives get exposed - the most confidential information gets sold. I really understand the sense that people seem to have that secure information is not really secure. That’s just speaking in the political sense, never mind other issues such as network security. You can give me all the information about how secure this is, but every time I turn around public data is being compromised by a prisoner or three million bank records have been hacked. (S_7)

Several subjects were not as concerned with the security of network infrastructure and related technologies as Subject S_7. Subject S_9 described how NASA and various university research centers provide very secure and encrypted information technologies dedicated to those interested in sharing aviation safety information. In agreement with Subject S_9, Subjects S_1, S_2, S_3, S_6, and S_{10} described how individuals and organizations handle collected data as the prime threat to disclosure or breeches in confidentiality.[28] As

---

[27] Subject S_2 described how many governments in the Middle East have agencies monitoring and reporting all Internet traffic within their society.

[28] Subjects S_1 and S_3 described different cases where individuals having access to a highly secured information sharing systems divulged content from databases. These incidents, related to both aviation

relayed below, this concern is even more problematic in smaller nations, where it is "easier to track and identify sources of information" (S_3),

> Databases with incident reports in small countries have a big problem. The number of pilots is usually small; one misspoken word about an incident will spread in hours throughout the aviation community. Even if you de-identify the report, some people will know who the pilot was. (S_3)

Subject S_3 also suggested that aviation safety information sharing systems should provide employees of participating companies with ways to submit information without being identified. This subject suggested strategies such as off-site communication facilities, Web access, and separate telephone lines (S_3).

Subjects indicated that airlines or other organizations (e.g., manufacturers, airports, etc.) are also concerned with filtering content to remove possible reference to their identities. Information describing brand names of equipment, geographic locations, and unique operational processes were examples of information that may be filtered from aviation safety information (S_2, S_4, S_5). Subjects S_2 and S_{10} also indicated that employees may refrain from sharing information out of fear of disclosing the identity of colleagues or affiliations. Sharing information may lead to negative financial, legal, or competitive consequences for individuals, companies, or other associations (S_2). These factors further diminish the ability of stakeholders to establish environments of trust.

All subjects believed that varying levels of trust between stakeholders hindered the ability to implement successful global aviation information sharing systems. Trust was emphasized as a key concern related to individual, cultural, and organizational relationships (S_2, S_3, S_4, S_5, S_7, S_{10}). Subject S_2 stated "competition" and "fear of the

---

security and safety, created a barrier to continued sharing of secured information between various government agencies and individuals.

public's perception of an airline's safety record" as two reasons companies are reluctant to trust each other with shared information. As a result, "airlines tend to give you what they want to give you, and not everything they have" (S_2). Subject S_3 shared a European perspective describing these concerns.

> In our country, the resistance to implement an aviation safety information sharing system is throughout the aviation community. Nobody trusts the other person, institution, or company. One could find out that in another company a lot is going wrong. The airlines are only sharing information as long as this information cannot be used against them. But, an airline does want to know everything about other airlines.
>
> One "agenda" is that an organization or airline is receptive for any aviation safety information. The second, "hidden agenda" is: "do not tell me about aviation safety information." The customers [passengers] might misunderstand our effort by believing we are not safe. (S_3)

Airlines tend to hold back information that may lead to false or misunderstood conclusions or financial or legal harm (S_2, S_3, S_4, S_7). Airlines are primarily concerned with jeopardy resulting from misunderstandings or misinterpretations of disseminated safety information. An aviation lawyer (S_7) provided the following assessment of airlines refraining from sharing information that may have negative implications,

> I think that there is an overriding, sort of, political, I don't know what the right word for it is, a sense that you don't want to admit mistakes in public in a way that other people can misconceive. (S_7)

Subject S_2 and S_4 identified relationships of public perception and government ownership of national airlines as a major deterrent to diffusion. According to Subject S_2, governments that own national airlines are just as concerned with negative perception by the public as privately owned airlines,

> I don't think many of these governments will allow individuals to report or share their safety related concerns. They don't want a bad reputation! So, I

> think that GAIN or other information sharing programs will be resisted, especially from parts of the world like the Middle East and China. In many of those types of countries, everything is "hush-hush." (S_2)

Other subjects described cultural values related to public perception that deterred the sharing of aviation safety information. Subjects S_3, S_4, and S_{10} described that many cultures view the admission of error as unacceptable social behavior. Subject S_{10} indicated that in some cultures of the Far East, admission of problems or errors may lead to punitive actions, such as fines or loss of employment. Subject S_3 offered the following insight related to German cultural norms and the sharing of aviation safety information,

> In Germany, no entities or individuals would support aviation safety information sharing efforts. This has to do with the "Germanic" culture and history. Germany was until 1945 a country without democratic tradition. This lead to a "military-type" attitude in companies and within the society, called *Schadenfreude*, meaning "to be happy that somebody else is at fault." (S_3)

Subjects S_2, S_3, S_4, and S_5 commented that most cultures value the profession of an airline pilot as a respected or "prestigious" (S_4) position requiring superior performance. Therefore, many cultures view disclosure of safety concerns by pilots as self-admission of inferior qualities or professional abilities (S_2, S_3, S_4, S_5). In some cultures, admission of safety concerns, even where no regulatory or operational violation exists, may cause pilots to lose income, job security, or even face imprisonment (S_2, S_3, S_5, S_8).

According to subjects S_2, S_3, S_4, and S_{10}, fear of public perception coupled with potential retributions by the company or legal actions tend to cause pilots to resist sharing safety information unless it is with a trusted colleague. An airline pilot (S_4) stated that pilots generally seek to solve problems on their own or with a trusted colleague before reporting the information to a safety system. However, Subjects S_4, S_8, and S_{10} expressed that various aviation safety information sharing systems such as FOQA, ASAP, and a number of airline owned networks have recognized increases in participation by pilots as sources of information. Over time, these systems demonstrated to pilots and airlines that participation is non-punitive and that individual identities are kept confidential (S_4, S_8, S_{10}).

Subject S_6 described that trust by stakeholders in policy and law is built through cases demonstrating the viability of these agreements in practice. According to Subject S_6, stakeholders need to see the agreements in writing and other evidence as described below,

> People need to see it demonstrated for them and hear from individuals that have participated in the program that they have been treated fairly. To do this, we try to be completely open with the pilots as to what the program will do and what it won't do. In training classes, I stand up and tell them, "Here's what can get you in trouble -- if you do this, don't come to me, because I don't have any choice about it." So we're trying to show them that we're not hiding anything from them. We are not going to try to get them suckered into reporting something and then somebody can turn around and get them for it.
>
> We also requested our senior pilots and pilots at other airlines that already had an established program to talk to our pilots and tell them how the program worked for them. Our pilots need to hear that other pilots reported something and I didn't get into trouble with the FAA.
>
> Our pilots must also learn from other pilots that there may be consequences – you know, they had some corrective actions they had to complete. We want them to know that the program is not a "get out of jail free card," but that they were protected from regulatory enforcement. That is the best selling tool we have! (S_6)

One of the most difficult challenges to implementing global aviation safety information sharing systems is establishing agreement by stakeholders to policies and law related to immunity (S_2, S_3, S_{10}). According to S_3, “Wherever in the world any aviation safety information sharing system is implemented, the first question will be about ‘immunity’.” All subjects indicated that policies offering immunity to sources of aviation safety information varied globally. Legal and cultural differences create barriers to developing uniform immunity policies. Subjects indicated that these policies were strongest and more commonly accepted when supported by national laws (S_3, S_6, S_7, S_9, S_{10}). However, Subject S_3 described how various CAAs attempt to maintain control of law related to immunity when negotiating in aviation safety information networks,

> I was a member of the “Legal Working Group” in GAIN. There was heavy competition between some of the CAAs over control of regulations and policies for giving violations to sources of information found to be at fault. This prevented a positive cooperation in legal matters and the distribution of aviation safety information. (S_3)

Establishing policy for immunity within organizations was also described as a challenge similar to regulatory concerns (S_1, S_2). As the following example demonstrates, internal policies related to immunity are required for successful diffusion of safety information,

> The problem with internal reporting systems at airports I have worked at is punishment for reporting problems. If there was a safety violation or concern, there was a tendency for the safety or risk management personnel to look for where the employee was at fault. This attitude often leads to deception by employees experiencing these safety concerns. (S_1)

Subject S_{10} added that changes in cultural value systems must occur before for policies or laws related to immunity become affective. The following discussion illustrates this concern,

> Individual airlines are having a hard time sharing information because the old school of thought was you get compliance through enforcement. The

> new way of thinking needs to be you get compliance through voluntarily sharing of information. If you make a mistake, you admit your mistake so that not only you learn from it but everybody else learns from it too. (S_{10})

Despite the aforementioned concerns, subjects indicated that airline stakeholders will likely share information if they trust in the information sharing system and their respective culture to protect their identity and guard against punitive actions (S_4, S_5, S_8, S_{10}). However, all subjects in the study identified diminished trust in the ability of different cultures to protect shared information from disclosure as a fundamental barrier to facilitating global aviation safety information sharing systems.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "trust, culture, and immunity."

1. Develop and implement ways to manage trust among stakeholders that will enhance the dissemination of aviation safety information.
2. Determine strategies and processes demonstrating long-term ability of information sharing systems or networks to uphold represented policies, laws, and regulations ensuring confidentiality and offering protection from liability or prosecution.
3. Determine strategies and processes that minimize the potential for negative perception by the public resulting from the dissemination of aviation safety information.
4. Identify cases or examples demonstrating the viability of laws or policies supporting conditions of immunity.

5. Utilize appropriate stakeholders to personally communicate cases or examples demonstrating the viability of laws or policies supporting conditions of immunity.
6. Determine strategies and tactics that enhance cultural values, policies, and laws offering immunity to sources of aviation safety information.
7. Identify and maintain awareness of potential risks from disclosure to stakeholders providing aviation safety data or information.
8. Develop agreements and understandings related to trust and confidentiality among varying cultures participating in aviation safety information sharing systems.
9. Evaluate and implement strategies and processes for de-identifying collected data such that sources to the data may not be identified.
10. Evaluate and implement strategies and processes for securing collected data such that sources to the data may not be identified.

Learning and feedback.

Airlines are hesitant to disclose examples of improvements in aviation safety resulting from sharing information (S_3, S_{10}). According to Subjects S_3 and S_{10}, there are two reasons for this stance. First, it is difficult to track and correlate the direct impact of shared safety information on aircraft operations and pilot performance. While the impact of some shared information on flight safety is clear (e.g., regulations, maintenance directives, etc.), it is difficult to collect and measure how diffused safety information is used by industry stakeholders and whether that use led to improved safety (S_3). Secondly, the public reacts negatively to proclamations of improved safety, since these statements are often interpreted as an admission of existing safety problems (S_3, S_{10}).

Internally, airlines provide opportunities for learning and feedback. Subject S_3 observed that pilots tend to be more receptive to learning from other pilots within their own organization.[29] In general, Subject S_3 believed that pilots of all cultures prefer reading safety bulletins as a way to seek information or new knowledge related to aviation safety. Many airlines create safety bulletins that are distributed to all pilots and line personnel within each organization (S_8). These bulletins contain information from many internal and external sources. The bulletins provide "analysis with conclusions presented in an organized format" (S_8). In the case of Subject S_8's airline, readers are provided with ways to submit feedback related to information contained in each bulletin.

Subject S_{10} agreed with the importance of providing feedback to industry stakeholders. Feedback should include information describing what types of data have been collected, how the data has been processed and used in the work environment, and the results of using the data (S_{10}). According to Subject S_{10}, managing feedback is a critical step in sharing aviation safety information,

> The greatest challenge related to feedback is getting it to the people who can really use it – those that can use it to prevent the same mistakes from happening again. Feedback is the real thing I think we still need more work on; otherwise, all we're doing is collecting data, and that doesn't do anyone any good. (S_{10})

Subjects provided little information regarding the collection and dissemination of aviation safety information by airlines indigenous to underdeveloped countries. Subject S_7 suggested that pilots of underdeveloped countries may indirectly benefit from knowledge held by major airlines, if these pilots participate in training offered by major

[29] Subject S_3 indicated that U.S. pilots seem to be more receptive to sharing safety information with each other, and openly exploring safety issues, than pilots of other cultures. Subject S_3 stated, "Some U.S. pilots will take extra simulator hours to find out how his aircraft flies without rudder, engines, and ailerons. But this behavior is restricted to Americans only, no other society I know of permits this type of learning."

airlines. None of the subjects was aware of any programs dedicated to disseminating safety information to airlines of underdeveloped countries.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "learning and feedback."

1. Determine and implement strategies and processes for tracking and disseminating case examples, applications, or best practices resulting from the use of shared aviation safety information.
2. Determine and implement strategies and processes for pilots to provide mentorship or interact and share information.
3. Produce and disseminate safety bulletins that summarize relevant issues and processes, provide recommendations, and enable feedback from stakeholders.
4. Consider ways to distribute safety bulletins to various national airlines – especially those not capable of tracking and disseminating safety information.

Technology and human interaction.

Concerns related to technology and the diffusion of aviation safety information were expressed by many of the subjects. Subject S_1 stressed that industry stakeholders need to standardize formatting and hardware protocols used to network databases containing aviation safety information. According to Subject S_1, various U.S. government agencies maintain open databases without providing software to read the data or metadata to understand the coding. Several subjects suggested that all sources of aviation safety data should be published in formats easily retrieved from the Web (S_1, S_3, S_4, S_6, S_8, S_9).

Web interfaces enabling remote uploading and access to searchable safety information was recommended by Subjects S_3, S_4, and S_8. Subjects S_3 and S_4 listed characteristics that should be inherent to all Web sites used to collect and disseminate aviation safety information.

1. Access and login processes should be time-efficient and easy to execute.
2. Web interfaces should clearly identify what types of information can be uploaded or retrieved.
3. Navigation should be very easy to understand and accomplish.
4. Data or information fields should provide opportunity to upload unstructured information about any relevant topic.
5. Available information should be archived, kept open to access, and not moved or deleted.
6. Methods for searching the Web site should be apparent, effective, and efficient.
7. Interaction with features on the site should be time-efficient and data transfer rates should be fast. (S_3, S_4)

As airline pilots, Subjects S_4 and S_5 also noted frustration with processes and technology used to report safety issues. Subject S_4 described that technology used to report safety issues was sometimes difficult to use and not always the preferred medium,

> Most pilots would rather go into the office and say, "Hey, this is my issue and can you take care of it and fill out the report?" Reports are lengthy and time consuming and don't always fit the issue. They will ask time and date and location, but if you just want to fill out certain information, you can't. People get frustrated. I have to fill out this block on the form - because if you don't, then when you "hit enter" it'll say you didn't do this block, and that, of course, makes everyone angry. It's not all that user friendly. I

> think everybody would rather just have an office they could come into and complain. (S_4)

Becoming overly reliant on automated processes and technologies without providing opportunity to include expert advice or analysis was also described as a barrier to diffusion (S_4, S_7). Subject S_7 offered the following observations relating technological interpretation of data and expert intervention,

> I'm interested in how humans put a gloss on reality and how they decide on what happened. So, rather than taking as gospel truth a spreadsheet or a matrix, this number of events, this links this to this, I'm more interested in saying, "Well, who decided that? How do you know that? Who made that decision to put that piece of data in that box?" Having meetings with people who know about what went in the box is probably more useful than saying, "okay, you're granted some sort of security access and we'll give you data then you can run a statistical analysis." That it ends up as numbers or written descriptions on a piece of paper or a spreadsheet. It [the data] had to get there from somewhere. So, certainly having the human involved where people can talk about it and kick things around and have access to the information, strikes me much more important than saying, "we can share things electronically, we're going to move files around and I can data mine it in some mathematical way, for example, or look for correlations or patterns from a small sample to a large sample. (S_7)

Subject S_4 also suggested the importance of including experts in the analysis of data. This subject described a case where FOQA data indicated a significant frequency of pilot error at a major airline. Once examined by experts, it was determined that the data reflected an error in a mandated procedure that pilots were correctly executing. According to Subject S_4, this example demonstrates why pilots are sometimes reluctant to provide information. Pilots fear that they will be held accountable for situations that have been incorrectly assigned, processed, or interpreted (S_4).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "technology and human interaction."

1. Determine best practices for standardizing technology related formats and protocols used to disseminate aviation safety information.
2. Publish instructional information and processes for stakeholders desiring to use electronically published aviation safety information.
3. Usability of technological infrastructure should be analyzed and designed to meet the needs of stakeholders.
4. Processes, analyses, and outcomes generated from automation must allow opportunity for expert human intervention and interpretation.
5. Consider alternative processes to technology for collecting information that are less impersonal, restrictive, invasive, or demanding.

Networks of practice.

Using GAIN as an example, subjects were asked to describe barriers to the diffusion of aviation safety information related to global networks of practice. In response, many of the subjects reiterated issues described in the sections above as determents to diffusion within networks of practice. Furthermore, discussions with subjects revealed little support for global networks of practice dedicated to aviation safety information sharing.

All of the subjects described differences in cultural values as a significant barrier to the diffusion of aviation. Subject S_{10} stated that variations in national and organizational cultures, “prevent everyone from getting on the same page” in terms of agreeing to standards and willingness to share information. This subject added that it is “difficult enough to do that with companies in our own country, and when you get outside our country, there are a lot more barriers” (S_{10}). In agreement with these assessments, Subject S_3 indicated that “no networks exists that are able to share good safety information across different cultures.” Subject S_1 characterized various national stakeholders facilitating domestic and international networks of practice as individuals with “stubborn belief systems,” and therefore unwilling to negotiate or compromise on issues that would facilitate diffusion within and across various networks.

Subjects S_1, S_3, S_4, and S_8 also described that individuals facilitating aviation safety information sharing networks usually have little understanding of processes related to the diffusion of information or knowledge. Subject S_3 explained this situation in the following interview excerpt,

> Only a fraction of those people who run aviation information systems understand the philosophy behind them. The rest are just doing the tasks assigned to them. However, the philosophy is not understood by them. This is not the fault of these people. Sharing aviation safety information is a very complex subject, which needs more than “understanding,” it is a hard and long-lasting task to learn. (S_3)

In addition to deficiencies in expertise by stakeholders implementing networks of practice, Subject S_7 suggested that motivation by stakeholders to these networks may also be less than needed to ensure a successful network. According to Subject S_7, low motivation may be partially caused by the tradeoffs between perceived benefits for establishing aviation safety information networks compared to the complexities of creating these systems. Subject S_7 also suggested that societies may have low motivation to implement these networks successfully, since these initiatives may not directly correlate with saving lives,

> I think the goal is well worth doing, but it seems like the benefits that could be realized by something like GAIN get lost in the problems that it takes to create the system. Fortunately, airplane accidents are rare enough -- system problems and equipment failures and procedural mistakes and piloting errors aren't all that rare, but the bad outcomes are quite rare. In world-wide aviation, deaths are fairly few and far between. So, there may not be a lot of push to say we can really save lives if we do this. It's not like, for example, information sharing about rare diseases. Those sorts of information sharing systems are really up front about saving lives. (S_7)

Subject S_8 agreed that goals associated with networks such as GAIN are worth pursuing. However, this subject believed that the concept of a global network of practice would create "chaotic and messy databases" containing data or information that would "barely resemble what's really happening in the real world" (S_8). For these reasons, Subject S_8 recommended that diffusing aviation safety information is best facilitated through alliances negotiated between various industry stakeholders. Subject S_8 provided the following rationale for this argument,

> Frankly, I wonder what's so positive about amalgamating and sharing data, can someone explain that to me? What's the positive of that on a multi-company level rather than just having the data in silos at the individual carriers with a line to contact your counterparts at the other carriers if you want to know anything about an area they operate in or have a safety issue with? (S_8)

Subjects described alliances as similar to communities of practice. These descriptions and related issues are described in the following section.

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the theme of "networks of practice."

1. Determine possible solutions to variations in national and organizational cultures that deter the diffusion of aviation safety information within and among networks of practice.
2. Determine possible solutions to variations in database structures and other technological infrastructures that deter the diffusion of aviation safety information by participants to networks of practice.
3. Determine strategies for hiring or training human resources qualified to facilitate networks of practice or alliances.
4. Consider strategies and processes for motivating stakeholders to support and participate within networks of practice.
5. Evaluate benefits and detriments to establishing networks of practice requiring negotiated conditions and requirements for stakeholder participation.

Alliances and communities of practice.

Subjects S_2, S_6, S_8, S_9, and S_{10} provided examples of alliances formed to facilitate sharing aviation safety information. Subjects described these alliances as negotiated agreements among stakeholders to share or advocate the sharing of aviation safety information. These subjects viewed alliances as an effective way to negotiate and solve issues and barriers related to sharing information within and among companies and other industry stakeholders. Subject S_8 added that alliances were useful in screening data and reducing information overload. All of these subjects agreed that alliances are more effective in negotiating agreements and establishing standards and policies than global networks of practice.

Subject S_6 described one alliance as consisting of several of the largest international carriers, along with several of the smallest carriers. These types of relationships are possible, since negotiated alliances help to reduce barriers such as competitive concerns and fear of disclosure related to sharing information (S_8, S_{10}). Subject S_6 added that alliances have been effective in increasing trust by participants. Alliances increase trust by working directly with government and legal agencies to solve concerns related to disclosure and other regulatory concerns (S_6, S_9). Alliances have also provided teams of individuals who will advise other industry stakeholders on best practices for establishing aviation safety information sharing systems or networks (S_6, S_9).

Airline industry alliances are communities of practice established to enhance the diffusion of aviation safety information (S_3). According to Subject S_3, as communities of practice, alliances have been more successful in the U.S. than in Europe or many other areas of the world. The relative lack of success in Europe with alliances was attributed to greater variance in cultures, predominance of government-owned airlines, and greater frequency of geopolitical systems (S_3, S_{10}).

Examples of alliances referred to by subjects included well-known programs such as the aforementioned Aviation Safety Action Programs (ASAP), the Line Operations Safety Audit (LOSA) program, and many privately arranged alliances that may not be publicly known (S_6, S_8, S_9, S_{10}).[30] Alliances may or may not have government participation or funding (S_6). The purpose of each alliance is dynamic over time and can be negotiated to meet the specific needs of different partnerships (S_6, S_9).

[30] Subject S_8 indicated that, "we [an international airline] are involved in so many safety information sharing alliances that it is hard to remember the names of all of them."

Subject S_8 stated that alliances enable face-to-face collaboration in order to determine ways to "gather, collect, collate, track, trend, and extract data out of safety reports in a logical manner." All interview participants indicated face-to-face meetings as perhaps the greatest benefit to alliances – especially in regards to collecting data and information from pilots.

Many participants emphasized the benefits to interviewing pilots participating within alliances (S_2, S_3, S_5, S_6, S_8, S_9, S_{10}). Examples of key points made by a few of these subjects are stated below,

> It is necessary to give a pilot the chance to talk about their experiences - in an open manner. When they can describe the problems they had to another person, they will be open to learning and sharing other information or perhaps advice. This is a two-way "business." (S_3)

> We really want to know about the exact details of what the pilot reported. Talking with pilots helps us to find out about continual problems or procedures everybody knows could be better, but that we've been doing so long, everyone just forgets to complain about it. (S_6)

> Having meetings and face-to-face interactions with pilots helps to build their trust; and, I think is also a better way to get information than a computerized system. (S_2)

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the theme of "Alliances and communities of practice."

1. Evaluate and compare potential benefits and barriers to diffusion resulting from participation in communities or alliances of practice.
2. Determine strategies and processes for establishing communities of practice or alliances.

3. Determine strategies and processes for communities or alliances of practice to enhance the diffusion of aviation safety information.
4. Determine strategies and processes for communities or alliances of practice to serve as advocates to other aviation safety information networks, systems, government agencies, or airlines.

Immunity and alliances.

Alliances that included government agencies were cited as potentially favorable to establishing immunity and maintaining trust of stakeholders to aviation safety information sharing systems (S_1, S_6, S_9). Subjects S_1 and S_6 described several cases where the U.S. Secret Service and the U.S. Transportation Security Administration attempted to identify and punish participants in ASAP for operational violations. According to Subject S_6, the FAA upheld their agreement to protect participants in ASAP from prosecution, and were able to block these agencies from pursuing their cases against the ASAP members. This resulted in a significant increase of trust by U.S. pilots in the ASAP program.

Subjects S_6 and S_9 also provided cases where various government agencies worked with alliances to help analyze and solve safety related problems. In many of these cases, government agencies agreed to policies of immunity. According to Subjects S_6 and S_9, this type of relationship between government agencies and alliances lead to solutions for many of the safety problems investigated.

Cases were presented describing potential conflicts between government and alliances. Subjects S_6 and S_9 described how in one U.S. alliance, confidential data would be stored and protected in a database owned by NASA. In this case, the alliance determined that the U.S. National Aeronautics and Space Act would protect the aviation safety data stored at NASA (S_9). The National Aeronautics and Space Act provides indefinite protection from disclosure of data or information used for research and collected by NASA from non-Federal sources (Report of the Committee on Commerce, Science, and Transportation on S. 342, 1999).[31] According to the following discussion by Subject S_6, the FAA took a different position regarding the ownership and access to the data provided by the alliance to NASA,[32]

> When the data was going to be housed at NASA, everyone said, great idea, count us in. Then, word came down from the FAA that at the end of 2 years they think they should own that database. The FAA told us that they have been given the responsibility by Congress to oversee the airspace system. And so, they believe that they have the responsibility to own this data. (S_6)

Subject S_{10} described tenuous situations of how various national agencies had agreed to, but did not follow policies in various programs. Some of these governments agreed to participate in alliances as an opportunity to discover violations as a hidden agenda. Once discovered, these agencies proceeded with penalties against those identified as responsible, even after agreeing to support policies of immunity (S_{10}).

Both government agencies and companies participating in alliances must establish policies and processes related to immunity for employees sharing aviation safety

[31] The National Aeronautics and Space Act also provides specific protection from disclosure resulting from inquiries made through the FOIA (Report of the Committee On Commerce, Science, And Transportation on S. 342, 1999, Title III - Miscellaneous Provisions).

[32] At the time of this writing, and according to Subjects S_6 and S_9, the alliance, NASA, and the FAA were still debating this situation. Both subjects indicated it was the intention of the alliance to proceed with contributing the data to NASA.

information (S_2, S_3). Subject S_2 made the following observation in concern of retribution to participating employees by employers,

> If you got into the system and gave information, then the company probably knows who you are. The problem is, you are giving out "company property information" and you may be subject to disciplinary action or even termination for saying, "We took off today with some sort of an engine problem." This kind of stuff needs to be known, but the company can't be allowed to go after you or violate you. (S_2)

According to some of the interviewees, policies regarding immunity must be clear and well communicated (S_2, S_3, S_5). Subject S_3 indicated that some aviation sharing information systems have, "marketed their policies of immunity to be more protective than they really are." This subject indicated that stakeholders are often confused over concepts such as "limited" or "partial immunity" and "total immunity." According to Subjects S_2 and S_3, alliances with government partnerships sometimes advertise total immunity to participants when regulatory agencies only extend limited immunity. These situations have reduced the trust of pilots toward aviation information sharing systems offering immunity (S_5). Alliances should work to negotiate written contracts with government agencies and organizational management ensuring various levels of immunity to stakeholders to the alliance (S_3).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "alliances and immunity."

1. Evaluate potential benefits and risks associated with government agencies serving as partners to alliances.
2. Establish internal policies and agreements facilitating immunity to employees of government agencies and other organizations serving as stakeholders to alliances.

3. Clearly state and communicate policies and conditions of immunity to alliance stakeholders.
4. Alliances should consider negotiating agreements, policies, and laws related to immunity with government or legislative agencies.

Networks, databases, and alliances.

Subjects $S_{1,}$ S_2, S_3, and S_9 suggested that alliances should use a centralized database for information released to the public. These subjects believed that stakeholders to the database should solicit de-identified and voluntarily contributed data or information from existing networks or alliances. This type of database and network architecture would potentially help to protect sources, reduce information overload, help establish standards, and enhance dissemination of collected aviation safety information ($S_{1,}$ S_2, S_3, S_9). According to Subject S_2, "networks should join together to support the database as a service to the industry." This database of aggregated aviation safety information should be designed for open access to the public (S_1, S_3). Subject S_1 described this concept in the following discussion,

> There needs to be a centralized database that takes the facts of each incident, identifies the key elements in the incident (why it happened, how it happened, etc), and the lessons learned. This database needs to be accessible by those in the industry, not just those with a security clearance. The security clearance often provides a barrier to those who are trying to use the data to help make the industry safer. (S_1).

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the linked themes of "alliances, networks, and databases."

1. Evaluate participation in an open access centralized database established for collection of voluntarily submitted and de-identified data contributed by alliances, networks, or other organizations.

Legislative Acts.

Interviewees provided little information regarding issues of disclosure and national legislative Acts such as the USA Patriot Act and Freedom of Information Act. Subject S_6 stated, “we have not seen any fallout from any of those Acts.” Subject S_7 believed that these types of government policies could pose a threat to information sharing systems in their ability to protect the identity of sources. According to Subject S_7, “we do not know enough yet about how these Acts may interact with safety information programs.” Subject S_7 added the following discussion as an example of this problem,

> Section 1520 of Title 49 of the Code of Federal Regulations refers to sensitive security information. It says, you may not release that information but then the next statement is, except as deemed appropriate by the Under Secretary of Department of Homeland Security [DHS] or possibly a response to a valid subpoena, then it will be reviewed by the DHS. So, my perception is it would be impossible under the law to keep anything absolutely confidential unless it’s maybe to the level of a state secret or a CIA intelligence bulletin -- but ordinary government process is not always confidential. There are mechanisms by which you can legitimately ask for information. There actually are provisions and regulations that tell you that information can be available to you if they choose to release it to you. (S_7)

Subjects S_2 and S_3 described information policies and related Acts used in other nations. They provided examples of how various levels of protection from disclosure are based on the culture’s classification system for types of information (e.g., scientific, legal, business, etc.). Subject S_3 explained that some cultures will protect disclosure of sources if they disseminate information to universities, lawyers, or doctors. Unlike the U.S., many cultures do not provide any agreements related to immunity resulting from participation in aviation safety information sharing systems (S_2, S_3). Subject S_3 noted national law and polices related to disclosure and immunity in the following dialog,

> Within our country, you can send safety information to an aviation safety sharing system about various working conditions related to your employer. This information will not be analyzed, it will be destroyed. The employer may fire the employee by just suspecting that he or she has given company secrecies to the information system. This is called a suspected "breach of contract" within our culture. The aviation information system will not disclose names of the reporter, under no circumstance. If the system were to do so, the flight crew reporting the information could be sentenced to at least two years jail (breach of secrecy). (S_3)

From the above evidence, the following ontology was interpreted and added to the taxonomy. The ontology is subordinate to the theme of “legislative Acts.”

1. Maintain awareness of and evaluate national legislative Acts that may threaten or impede the diffusion of aviation safety information.

Table 13 summarizes the results of the taxonomy and ontology interpreted in the second sub-problem. The taxonomy and related ontology represent a model of issues related to disclosure and policy that may affect the diffusion of aviation safety information within and among communities or networks of practice. This model is used in the third sub-problem as the foundation for developing potential solutions to policy issues in public disclosure that act as barriers to the diffusion of aviation safety information.

Table 13. Taxonomy and Ontology of Diffusion, Disclosure, and Policy Issues in Aviation Safety Information Sharing Systems

Taxonomy	Ontology
Information overload	Determine processes to manage and analyze information internal to the organization prior to participating in external information sharing systems
	Determine problems to be solved and types of information needed prior to collecting or sharing new information
	Develop effective and efficient methods to disseminate information and align these processes with the needs of stakeholders using the information
	Develop ways to structure and present information that will facilitate effective and efficient usage by stakeholders
Databases and standards	Maintain and publish directories of all known aviation safety information sharing systems, networks, or databases
	Catalog metadata describing technologies, standards, and data relevant to each known aviation safety information sharing system, network, or database
	Evaluate the feasibility and benefits for developing or sharing information with centralized industry sponsored database systems
Data mining and semantic analysis	Supplement expert analysis and semantic interpretation of aviation safety information with data mining tools
	Select data mining applications viable to development of taxonomy and related ontology

Table 13 (continued).

Taxonomy	Ontology
Taxonomy and ontology	Allocate time and expert resources for developing taxonomy and ontology
	Develop taxonomy and ontology as a framework for collecting and disseminating future data or information
	Consider the affect of cultural values on semantic meaning when reconciling or developing taxonomy and ontology
Search strategies	Provide time and access for stakeholders to conduct face-to-face meetings or attend industry conferences related to aviation safety
	Seek or develop search tools and related strategies for individual stakeholders that will enhance retrieval of needed aviation safety information
	Seek or develop search tools and related information technologies enabling storage and retrieval of aviation safety information disseminated in varying formats of structured and unstructured data
Trust, culture, and immunity	Develop and implement ways to manage trust among stakeholders that will enhance the dissemination of aviation safety information
	Determine strategies and processes demonstrating long-term ability of information sharing systems or networks to uphold represented policies, laws, and regulations ensuring confidentiality and offering protection from liability or prosecution
	Determine strategies and processes that minimize the potential for negative perception by the public resulting from the dissemination of aviation safety information

Table 13 (continued).

Taxonomy	Ontology
Trust, culture, and immunity	Identify cases or examples demonstrating the viability of laws or policies supporting conditions of immunity
	Utilize appropriate stakeholders to personally communicate cases or examples demonstrating the viability of laws or policies supporting conditions of immunity
	Determine strategies and tactics that enhance cultural values, policies, and laws offering immunity to sources of aviation safety information
	Identify and maintain awareness of potential risks from disclosure to stakeholders providing aviation safety data or information
	Develop agreements and understandings related to trust and confidentiality among varying cultures participating in aviation safety information sharing systems
	Evaluate and implement strategies and processes for de-identifying collected data such that sources to the data may not be identified
	Evaluate and implement strategies and processes for securing collected data such that sources to the data may not be identified
Learning and feedback	Determine and implement strategies and processes for tracking and disseminating case examples, applications, or best practices resulting from the use of shared aviation safety information
	Determine and implement strategies and processes for pilots to provide mentorship or interact and share information
	Produce and disseminate safety bulletins that summarize relevant issues and processes, provide recommendations, and enable feedback from stakeholders

Table 13 (continued).

Taxonomy	Ontology
Learning and feedback	Consider ways to distribute safety bulletins to various national airlines – especially those not capable of tracking and disseminating safety information
Technology and human interaction	Determine best practices for standardizing technology related formats and protocols used to disseminate aviation safety information
	Publish instructional information and processes for stakeholders desiring to use electronically published aviation safety information
	Usability of technological infrastructure should be analyzed and designed to meet the needs of stakeholders
	Processes, analyses, and outcomes generated from automation must allow opportunity for expert human intervention and interpretation
	Consider alternative processes to technology for collecting information that are less impersonal, restrictive, invasive, or demanding
Networks of practice	Determine possible solutions to variations in national and organizational cultures that deter the diffusion of aviation safety information within and among networks of practice
	Determine possible solutions to variations in database structures and other technological infrastructures that deter the diffusion of aviation safety information by participants to networks of practice
	Determine strategies for hiring or training human resources qualified to facilitate networks of practice or alliances
	Consider strategies and processes for motivating stakeholders to support and participate within networks of practice

Table 13 (continued).

Taxonomy	Ontology
Networks of practice	Evaluate benefits and detriments to establishing networks of practice requiring negotiated conditions and requirements for stakeholder participation
Alliances and communities of practice	Evaluate and compare potential benefits and barriers to diffusion resulting from participation in communities or alliances of practice
	Determine strategies and processes for establishing communities of practice or alliances
	Determine strategies and processes for communities or alliances of practice to enhance the diffusion of aviation safety information
	Determine strategies and processes for communities or alliances of practice to serve as advocates to other aviation safety information networks, systems, government agencies, or airlines
Alliances, networks, and databases	Evaluate participation in an open access centralized database established for collection of voluntarily submitted and de-identified data contributed by alliances, networks, or other organizations
Legislative Acts	Maintain awareness of and evaluate national legislative Acts that may threaten or impede the diffusion of aviation safety information

Analysis and Findings for the Third Sub-problem

The third sub-problem analyzes GAIN as a case study. GAIN is presented within a thematic framework developed through descriptive analysis of the interpretations made in the first and second sub-problems. Correlations made in the third sub-problem were based on categorical pattern matching of content related to disclosure, policy, and diffusion. From these interpretations, potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information within GAIN's community and network of practice were interpreted, evaluated, and presented in the subsequent sections.

GAIN as a Case Study of Information Policy, Public Disclosure, and Diffusion

This investigator has described GAIN as a strategic alliance relevant as a case study in KM. The primary objective of GAIN is to facilitate the sharing of data, information, and knowledge used to improve safety within the airline industry. GAIN's conceptualization, implementation, and associated challenges have been documented in this study's review of the literature. A consistent and predominant challenge to the evolution of GAIN as a community and network of practice has been the negative impact of public disclosure on the diffusion of aviation safety information. The following themes address these issues and relate information policies that may serve as potential solutions to public disclosure as a barrier to diffusion of aviation safety information.

Developing and negotiating policies related to disclosure.

Developing and negotiating policies related to disclosure is ontology common to the taxonomies developed in the first and second sub-problems in this study. Policies or agreements regarding access and usage of publicly open sources containing de-identified data or information are relatively straightforward to implement. These types of sources (e.g., ASRS and the NTSB) have established policies and processes for treating disclosure issues when disseminating information. However, gaining access and embracing issues related to disclosure for privately owned or confidential sources requires careful negotiation and collaboration among all stakeholders.

In the book *Democracy by disclosure: The rise of technopopulism*, Graham (2002) provided cases in the health, food, transportation, and medical industries demonstrating collaboration and negotiation as key strategies for addressing issues related to public disclosure. In the medical industry, collaboration was shown to be essential to building non-punitive cultures. Graham also described the ability to negotiate collaborative environments as more important to enhancing diffusion than levels of confidentiality warranted by the reporting system.

In negotiating access to information, Graham (2002) recommended that levels of disclosure should be matched to risks. Levels of disclosure should be recognized as a continuum, with policies, "constructed to serve multiple purposes and reduce conflicts among values" (Graham, 2002, p. 155). According to Graham, this strategy is appropriate in environments where stakeholders cannot agree on the extent or ability to warrant confidentiality. Collaborative environments for sharing information are also dynamic in that policy related to disclosure can be frequently modified in order to protect the viability of the information sharing system (Graham, 2002).

Collaborative environments should employ or retain experts to help solve problems within or among communities of practice (Hildreth, 2004). Wenger (1998, p. 105) described the need for experts or "brokers" in communities of practice for facilitating interaction among individuals and objects. Personal identity is related to levels of interaction with communities or networks. Experts that broker participation of stakeholders often negotiate these levels of interaction (Wenger, 1998). As information experts, brokers help communities of practice negotiate the processes and policies used to disseminate information across cultural and technological boundaries. Brokers can help to negotiate processes of disseminating information, such as to the media or events that support face-to-face meetings (Hildreth).

GAIN Working Groups have investigated and described many issues related to risks associated with disclosure. These groups have also analyzed and cataloged disclosure policies for many industry stakeholders. Based on these observations and analysis, the following policy issues are recommended as potential solutions to this sub-problem.

1. GAIN should assist in developing collaborative environments that address issues related to disclosure within and among various alliances or networks seeking to share aviation safety information.
2. GAIN should offer expertise that will help stakeholders align and negotiate disclosure policies with associated risks. A systematic approach for renewal and adjustment of these polices should be supported by GAIN.
3. GAIN should establish qualified information professionals or brokers that can assist in negotiating levels of participation and disclosure within and among stakeholders to alliances, communities, or networks of practice.

De-identifying data and information.

The de-identification of data and information is a policy concern of public disclosure common to the taxonomies developed in the first and second sub-problems in this study. GAIN’s Working Group IV addressed concerns related to the de-identification of aviation safety information held in databases. De-identification is essential to building stakeholder trust. However, processes associated with de-identification may inhibit the ability to discover new meanings or patterns within the data that may lead to improved safety. Therefore, special processes and experts should be used to protect and retain the value of data that will be de-identified (Gupta, Saul, & Gilbertson, 2004).

Hernon, Relyea, Dugan, and Cheverie (2002) recommended that organizations concerned with de-identification evaluate software specifically designed to remove or protect the identity of individuals contained in electronic data files. Other authors recommended combining technological processes with expert analysis to “cloak” (Barth, 2004, p. 473) or de-identify personal or other confidential information (Douglass, Clifford, Reisner, Moody, & Mark, n.d.). Barth described these processes as applied to knowledge-based communities in commercial settings. Douglas et al. demonstrated a case utilizing experts and technology to de-identify confidential information contained in unstructured text.

GAIN has considered the need for processes and policies applied to the de-identification of data. However, GAIN should consider providing expertise to industry stakeholders regarding these concerns. Based on these observations and analysis, the following policy issues are recommended as potential solutions to this sub-problem.

1. GAIN should develop a community of practice designed to provide industry stakeholders with expertise and technologies useful in the de-identification of data or information.
2. GAIN should evaluate and demonstrate technologies to industry stakeholders that may be useful in de-identifying data or information.

Securing data, information, and privacy of communication.

Creating and implementing policy and processes related to securing data and information is a theme common to the taxonomies developed in the first and second sub-problems of this study. Securing information technology and related infrastructure is a core activity of knowledge management (Sahasrabudhe, 2000). Meadow (1992) described how securing data, information, and privacy of networks have and will continue to be primary concerns to facilitating communication.

Processes such as data encryption and establishment of firewalls are rudimentary examples of security applied to KM and communication systems (Meadow, 1992; Sahasrabudhe, 2000). Jamieson and Handzic (2003, p. 477) offered, “a framework for security, control, and assurance” related to KM. They describe risks and strategies for controlling security related to hardware, software, systems, applications, human resources, and networks in the KM environment (Jamieson & Handzic).

GAIN has considered the need for processes and policies applied to securing data, information, and the privacy of communication. GAIN should consider providing expertise to industry stakeholders regarding these concerns. Based on these observations and analysis, the following policy issues are recommended as potential solutions to this sub-problem.

1. GAIN should develop a community of practice designed to provide industry stakeholders with expertise and technologies useful in securing data, information, and the privacy of communication.

2. GAIN should evaluate and demonstrate technologies and processes to industry stakeholders that may be useful in managing and balancing risks associated with controlling the security of data, information, and the privacy of communication.

Utilizing information policy and law related to disclosure.

Consideration of policies and laws related to disclosure is fundamental to several ontologies interpreted in the second sub-problem. The GAIN Government Support Team was established to investigate and evaluate information policies and laws that may affect the development of aviation information sharing systems. Information policies and laws related to disclosure are primary concerns to the implementation of GAIN's global aviation safety information sharing system. Legal or statutory concerns related to the diffusion of information have been documented in this study as key barriers to sharing aviation safety information.

Meadow (1992) has documented the long and extensive history of cultures attempting to control the diffusion of information through information policies. Information policy consists of interrelated laws, regulations, guidelines, and policy concerned with the life cycle of information (Hernon et al., 2002). The life cycle of information includes the creation, collection, storage, analysis, dissemination, and use of information. Those managing the dissemination of information must recognize that information policies and laws related to access, privacy, and security will probably affect each stage in the life cycle of information (Hernon et al., 2002).

Reconciling issues of disclosure with information policy and law is typically complex and not straightforward (Graham, 2002). Graham provided the following explanation for the generally complex and confusing nature of information policy and laws related to disclosure,

> Disclosure systems that aim to reduce risks have been products of expediency and frustration. Legislators have required organizations to reveal information to produce pragmatic compromises, correct market flaws, overcome perceived shortcomings of conventional regulation, and affirm core values. (2002, p. 11).

According to Graham (2002) and Marett (2002), information policies attempt to balance the risks of disclosure with varying cultural values sustaining a "right to know." Graham described interrelation of various cultural risks to the evolution of information policies in the following passage,

> Disclosure systems are inevitably products of the political process. They result from compromises that reconcile competing values and interests. Universally acclaimed in principle, disclosure often conflicts with protection of trade secrets, personal privacy, minimization of regulatory burdens, and guarding of national security. Compromises among such values can lead to fragmentation, distorted incentives, and excessive costs. In practice, communication, too, is complicated not only by political imperatives but also by cognitive distortions and the self-interested motivations of intermediaries who add their own interpretations. (2002, p. 16).

In his book *Information Law in Practice*, Marett (2002) suggested that information professionals should be concerned with analyzing and employing information laws and policies for managing the use and misuse of disseminated information. In agreement with Marett, Graham (2002) advised that information sharing environments managing disclosure as a means to reduce risks will require unique architectures of information laws and policies.[33] According to Graham (2002), these architectures evolve through political and administrative compromise. Information brokers or other intermediaries often negotiate these political and administrative

[33] Graham (2002, pp. 158-159) provided a taxonomy with ontology for considering the design of information architecture and policy applied to disclosure systems.

considerations concerning disclosure and related information policies (Graham (2002); Marett).

GAIN should serve as an intermediary providing expertise regarding information policy and disclosure. As a community of practice, GAIN should consider providing expertise to industry stakeholders regarding these concerns. Based on these observations and analysis, the following policy issues are recommended as potential solutions to this sub-problem.

1. GAIN should develop a community of practice serving as an intermediary helping stakeholders analyze, design, and manage varying architectures of information policies and laws related to disclosure.
2. GAIN should help industry stakeholders assess and reconcile information policies with risks associated with disclosure throughout the information life cycle.
3. GAIN should help industry stakeholders negotiate and manage political and administrative considerations related to the use and misuse of disclosed information.

Creating environments of trust.

This researcher has documented environments of trust as essential to the success of aviation safety information sharing systems attempting to manage risks from the disclosure of data, information, or knowledge. The First and Second GAIN Conferences identified establishing environments of trust as a key strategy for GAIN as a community and network of practice. Various GAIN working groups discussed developing policies and processes enhancing trust between stakeholders as a priority for successfully implementing GAIN's global aviation safety information sharing network.

Relationships of trust, culture, and the diffusion of aviation safety information or knowledge were predominant issues described by many of the subjects interviewed in the second sub-problem. All of the subjects interviewed stressed the importance of trust by stakeholders in policies and laws sustaining immunity from risks associated with disclosure.

Hildreth (2004) described the creation of trust between stakeholders as a key responsibility of communities of practice. Communities of practice should "determine the motivation and legitimation of the members, which in turn determine the identity and the trust and confidence of the members" (Hildreth, p. 73). According to Hildreth, the first task of a community of practice is to develop policies and processes that build relationships of trust among cultures and individuals. Once this is accomplished, stakeholders can then be encouraged to collaborate and share information (Hildreth).

Many authors such as Buckowitz and Williams (2000), Ford (2003), and Wenger, McDermott, and Snyder (2002) have provided guidelines, policies, and processes for building environments of trust within and among communities and networks of practice. Wenger, McDermott, and Snyder described case examples of communities of practice nurturing trust by building networks that attempt to solve shard problems. Utilizing knowledge brokers or intermediaries is also as a strategy for increasing trust when diffusing information or knowledge across boundaries (Wenger, McDermott, & Snyder). Within the context of KM and diffusion, Ford presented a taxonomy and ontology of concerns and recommendations for solving issues related to trust.

Suggestions to build trust have also included the development of non-disclosure policies and contracts (Magg & Flint, 2004) and “contracts of reciprocity” (Buckowitz & Williams, 2000, p. 196). Disclosure contracts or policies and contracts of reciprocity make explicit “fair processes” or “procedural justice” that will be followed in issues related to trust and the dissemination of information (Buckowitz & Williams, p. 196). According to Buckowitz and Williams, “Fair process builds trust and commitment, trust and commitment produce voluntary cooperation, and voluntary cooperation drives performance, leading people to go beyond the call of duty by sharing their knowledge and applying their creativity” (p. 196).

GAIN should serve as a community of practice and intermediary helping stakeholders create environments of trust. GAIN should provide expertise for developing contracts, policies, and processes that address concerns of disclosure specific in distribute communities and networks of practice. Based on these observations and analysis, the following policy issues are recommended as potential solutions to this sub-problem.

1. GAIN should serve as a community of practice and intermediary helping stakeholders create environments of trust.
2. GAIN should continuously develop and investigate policies and processes for managing trust as related to issues of disclosure within and among aviation safety information sharing systems.
3. GAIN should assist stakeholders in developing policies and contracts of fair process or procedural justice addressing issues of risks associated with public disclosure of aviation safety information.

Table 14 summarizes the results of the taxonomy and ontology interpreted in the third sub-problem. The taxonomy and related ontology represent recommendations for issues related to disclosure and policy that may affect the diffusion of aviation safety information within GAIN's community and network of practice.

Table 14. Taxonomy and Ontology of Diffusion, Disclosure, and Policy Recommendations Specific to GAIN's Community and Network of Practice

Taxonomy	Ontology
Developing and negotiating policies related to disclosure	Assist in developing collaborative environments that address issues related to disclosure within and among various alliances or networks seeking to share aviation safety information
	Offer expertise that will help stakeholders align, negotiate, and systematically renew disclosure policies and associated risks
	Establish qualified information professionals or brokers that can assist in negotiating levels of participation and disclosure within and among stakeholders to alliances, communities, or networks of practice
De-identifying data and information	Develop a community of practice designed to provide industry stakeholders with expertise and technologies useful in the de-identification of data or information
	Evaluate and demonstrate technologies to industry stakeholders that may be useful in de-identifying data or information

Table 14 (continued).

Taxonomy	Ontology
Securing data, information, and privacy of communication	Develop a community of practice designed to provide industry stakeholders with expertise and technologies useful in securing data, information, and the privacy of communication
	Evaluate and demonstrate technologies and processes to industry stakeholders that may be useful in managing and balancing risks associated with controlling the security of data, information, and the privacy of communication
Utilizing information polices and laws related to disclosure	Develop a community of practice serving as an intermediary helping stakeholders analyze, design, and manage varying architectures of information policies and laws related to disclosure
	Help industry stakeholders assess and reconcile information policies with risks associated with disclosure throughout the information life cycle
	Help industry stakeholders negotiate and manage political and administrative considerations related to the use and misuse of disclosed information
Creating environments of trust	Continuously develop and investigate policies and processes for managing trust as related to issues of disclosure within and among aviation safety information sharing systems

Summary of the Results

Summary of Results for the First Sub-problem

In the first sub-problem, a generalized taxonomy of KM that may be used to study global aviation or airline safety information sharing systems was developed. Data for treatment of the first sub-problem were publications purposively sampled for relevance to the definition, nature, foundation, or characterization of KM. Publications including KM case examples were also included as data. The resulting data set for the first sub-problem consisted of 134 documents published from 1995 to 2004. In addition to purposeful sampling strategies, the validity of the 134 data documents was qualified by reading and interpreting each document's content in relation to the domain of KM.

Semantic text-mining was used as an analysis for mapping linguistic units across words, sentences, and paragraphs within the 134 document data set. Data was analyzed using the software application *TextAnalyst* (see Appendix J). Text-mining was performed on the entire narrative within each document of the data set.

Semantic processing was first applied to all data files using *TextAnalyst's* default dictionary (see Appendix J). All combined data files consisted of 28,274 sentences. *TextAnalyst* identified 5,252 semantically significant nodes from the data set. Nodes were the basic unit of analysis in the first sub-problem.

The reliability of *TextAnalyst* in identifying nodes and related semantic weights was examined according to processes recommended by Popping (2000). The reliability of *TextAnalyst* was determined as exact when tested for multiple analyses using the same dictionary, software settings, and data set.

TextAnalyst's semantic validity was also examined according to processes recommended by Fattori, Pedrazzi, and Turra (2003) and Krippendorff (2004). A correlative analysis for validity was conducted on two data sets using *TextAnalyst*. Semantic weights for nodes associated with the theme of knowledge management from each data set were compared. The first data set consisted of definitions of KM published in the literature. The 134 data documents used for analysis in the first sub-problem represented the second data set. A correlation R statistic of .91 was determined after regressing the semantic weights of the concepts linked to KM in the data set with semantic weights of the same concepts found in the definitions of KM data set. This correlation was interpreted as (a) evidence the semantic validity of *TextAnalyst* was adequate and (b) further evidence that the context of the study data set was directly related to knowledge management and therefore valid for use in the first sub-problem.

A customized dictionary for use in *TextAnalyst* was developed. Default dictionaries usually contain basic vocabularies not related to problem solving in specific domains. Therefore, developing a customized dictionary was the first step toward building the taxonomy of KM. Development of the customized dictionary followed the procedures recommended by Krippendorff (2004), Neuendorf (2002), and Popping (2000). Meaning related to KM in the customized dictionary was developed and derived through thematic concept mapping. Thematic concept mapping is the process of developing and assigning meaning (themes) to nodes representing an expansive group of concepts or semantic relationships.

In this analysis, themes related to KM were identified and validated from (a) theoretical constructs related to the research problems, (b) concepts grounded in practice and documented in the literature, and (c) other concepts found semantically valid through text-mining and interpreted as related to the nature of the study. Dependent words or synonyms were also assigned to user specified words (themes) defined in the custom dictionary (see Appendix J). All interpreted KM related themes and dependent words used in the custom dictionary were validated for face validity by examining each term in the data as a key word in context.

Developing the custom dictionary required repeated text-mining processing as user words were interpreted or identified, categorized, and added to the dictionary. In this study, text-mining processing was repeated and results examined to interpret vocabulary hermeneutically and discover user words added to the customized dictionary.

Text-mining was applied to the data using the custom dictionary. With the exception of the theme knowledge, semantic weights increased for all other themes interpreted using the default dictionary. Knowledge had the highest semantic weight using the default dictionary. Therefore, knowledge decreased in semantic importance relative to increases in other thematic weight values using the custom dictionary. These increases suggest that the custom dictionary was useful in identifying and extracting additional meaning related to each theme related to KM.

A goal of this research was to develop a KM taxonomy focused on policy issues related to public disclosure that may affect knowledge diffusion. Therefore, knowledge management, diffusion, disclosure, and policy were analyzed in relation to concepts in the taxonomy. Ontologies related to knowledge management, diffusion, disclosure, and policy were interpreted from each theme’s semantic summary (see Appendix J). These processes and interpretations lead to the development of a generalized taxonomy of KM with related ontology. The taxonomy and ontology was subsequently used in the second and third sub-problems to investigate issues that may affect the diffusion of aviation safety information.

Summary of Results for the Second Sub-problem

The second sub-problem in this study was to develop a specialized taxonomy addressing issues controlling the diffusion of global airline or aviation safety information. Issues inherent to GAIN and other similar networks affecting the diffusion of airline safety data, information, or knowledge were identified, qualified, and compared to the generalized taxonomy of KM developed in the first sub-problem. These interpretative processes resulted in the development of a specialized taxonomy of KM related issues that may aid in the design and implementation of global airline safety information sharing systems.

Data used in the second sub-problem were interview transcripts obtained from stakeholders to GAIN and the global airline industry. Stratified purposeful sampling was used to select subjects for interview data collection. Ten subjects provided interview data for this sub-problem. All interview conversations were digitally recorded.

The ontology developed in the first sub-problem was used to derive a set of standardized open-ended questions for use in each interview (see Appendix U). Three experts validated the questions for clarity and face validity relevant to the problem statement. These questions served as a generalized framework for investigation during each interview.

Validity and reliability of the data used in the second sub-problem was established by (a) purposefully selecting subjects qualified as stakeholders to airline safety information sharing systems, (b) soliciting from subjects information and knowledge directly related to the ontologies developed in the first sub-problem, and (c) using the customized *TextAnalyst* dictionary validated in the first sub-problem. Semantic network analysis in *TextAnalyst* was used to further examine interview data (see Appendix J). All data content were reviewed for relevance to the taxonomy created in the first sub-problem.

Content analysis was conducted by reading and text-mining each interview data file. Interview data interpreted as relevant were extracted, sorted, and clustered in relation to the themes of diffusion, disclosure, and policy. Interpretive processes of indexing and pattern matching were used to correlate extracted interview data with existing themes or to discover new themes within the KM taxonomy.

Interview data was analyzed in relation to the themes of diffusion, disclosure, and policy within a thematic framework of KM created in the first sub-problem. Interpretative processes focused on identifying phenomena discovered in the data that may affect the diffusion of aviation safety information. These processes and interpretations lead to the development of a specialized taxonomy of issues related to diffusion, disclosure, and policy that may aid in the design and implementation of airline safety information sharing systems. This model was used in the third sub-problem as the foundation for developing potential solutions to policy issues in public disclosure that act as barriers to the diffusion of aviation safety information.

Summary of Results for the Third Sub-problem

The third sub-problem analyzed GAIN as a case study. GAIN was presented within a thematic framework developed through descriptive analysis of the interpretations made in the first and second sub-problems. Correlations made in the third sub-problem were based on categorical pattern matching of content related to disclosure, policy, and diffusion. From these interpretations, potential solutions to policy issues in public disclosure that prevent the collection and sharing of airline or aviation safety information within GAIN's community and network of practice were interpreted, evaluated, and presented in the third sub-problem.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Policy issues in public disclosure that prevent the collection and sharing of aviation safety information were identified and evaluated in this research. A generalized taxonomy with ontology of KM was interpreted and presented. This taxonomy may be used to identify and manage KM-related issues or methods affecting the diffusion of data, information, or knowledge within and among organizations and communities or networks of practice. A specialized taxonomy addressing issues controlling the information and knowledge diffusion of global airline safety information systems was also developed and presented. This specialized taxonomy may be used to manage issues inherent to GAIN and other similar networks that may affect the diffusion of airline safety data, information, or knowledge. The research was concluded by providing recommendations in policy for addressing public disclosure as a barrier to the diffusion of airline safety data, information, or knowledge.

Conclusions

Conclusions of the First Sub-problem

The first sub-problem in this study was to develop a generalized taxonomy with related ontology of KM. This sub-problem was successfully addressed in this research (see Table 11).

The interpreted taxonomy and ontology produced in this sub-problem represents a working model of KM. This model may be used to study global aviation safety information sharing systems, as well as other communities or networks of practice that wish to disseminate information across boundaries. The model establishes KM related issues or methods that potentially affect the diffusion of data, information, or knowledge within and among organizations or various communities.

The model of KM completed in this sub-problem was interpreted using deductive logic and constructivist strategies related to qualitative research. The model represents interpretations and conclusions as grounded theory based from evidence in the literature. The data used in these interpretations represented a thorough and encompassing review of literature describing the definition, nature, foundation, or characterization of KM as applied in the social world. Relevant themes were interpreted by examining the data in relation to the concepts of KM, diffusion, disclosure, and policy.

Text-mining was also used in this sub-problem as a strategy for triangulation applied to interpretative processes. Text-mining was used to help resolve and discover themes and relationships of KM related to issues in public disclosure that prevent the collection and sharing of data, information, or knowledge as documented in the literature.

Construct validity for interpretative methodology was established using the concepts of network of practice, community of practice, and best practices as representations of the social world. Network of practice, community of practice, and best practices were considered as boundaries to the interpreted KM taxonomy. Concepts and interpretations made under each of these categories were derived from issues related to policies, barriers, and disclosure that affect the ability of KM as a domain for managing knowledge diffusion.

The first hypothesis.

The hypothesis for this sub-problem was that issues related to KM that can directly affect the diffusion of data, information, or knowledge among organizations can be generalized as a taxonomy. A generalized taxonomy and ontology of KM was produced in this sub-problem (see Table 11). This taxonomy represents grounded theory developed from a comprehensive examination of examples and cases of KM contained in the literature. The taxonomy may be used to address challenges related to data, information, or knowledge diffusion in a variety of settings or domains. Therefore, the results of the research conducted in the first sub-problem support this hypothesis.

Strengths, weaknesses, or limitations of the research in the first sub-problem.

The prime strength of this analysis was the development of a generalized taxonomy of KM that may be used to help manage the diffusion of data, information, or knowledge. An additional benefit is that the taxonomy represents grounded theory based on interpretation of a comprehensive data set. This outcome should provide a platform of theory related to KM from which to conduct future research.

A weakness of this analysis was that a significant proportion of interpretation was based on the examination of semantic analysis produced through text-mining. Text-mining generates semantic relations of concepts derived from mathematical and statistical processing. These processes use a dictionary as a model for distilling concepts that may represent significant meaning in unstructured text (see Appendix J). Cases of relevant data were probably “lost” during processing, since meaning used in text-mining is limited to the construct of the dictionary and validity of algorithms used in the software. However, text-mining was determined as a valid and reliable method for developing generalized taxonomy induced from a large comprehensive source of data.

Conclusions of the Second Sub-problem

The second sub-problem in this study was to create specialized taxonomy addressing issues controlling the information and knowledge diffusion of global airline safety information systems. The specialized taxonomy was successfully developed in this sub-problem (see Table 13).

Standardized open-ended interviews were held with various industry stakeholders to collect data for this sub-problem (see Table 12). These stakeholders were purposively sampled to provide “knowledge, views, understandings, interpretations, experiences, and interactions” insightful to issues related to GAIN, public disclosure, and the diffusion of airline safety information (Mason, 2002, p. 63). Issues in the data inherent to GAIN and other similar networks that may affect the diffusion of airline safety data, information, or knowledge were identified, qualified, and compared to the generalized taxonomy of KM developed in the first sub-problem. Interview data was analyzed in relation to the themes of diffusion, disclosure, and policy within a thematic framework of KM created in the first sub-problem. Interpretative processes focused on identifying phenomena discovered in the data that may affect the diffusion of aviation safety information. These processes and interpretations produced a specialized taxonomy of issues related to diffusion, disclosure, and policy that may be used in the design and implementation of airline safety information sharing systems. The taxonomy, as presented in Table 13, with summarized ontology is presented below.

1. *Information overload*: Extensive volumes of existing data and information have created an environment of information overload within most medium to large airlines. Recommendations to address this problem include identifying the types of information needed and ways to diffuse that information within the organization prior to participating in external aviation safety information sharing systems. Airlines must also develop effective and efficient ways to structure, align, and disseminate information to meet the individual needs of stakeholders.
2. *Databases and standards*: Industry stakeholders are not usually aware of various databases and related standards used to collect, store, retrieve, and analyze aviation safety information. Most companies store aviation safety information in separate databases using different structures, taxonomies, or ontologies, and processes of analysis. Airlines should maintain and publish directories of known aviation safety information sharing systems, networks, or databases. Metadata and other relevant descriptions regarding technologies, standards, and data used in

each database or system should also be documented. It is recommended that airlines evaluate the feasibility and benefits for developing or sharing information with centralized industry sponsored database systems.

3. *Data mining and semantic analysis*: Processes for deriving interpretations or meaning of data related to aviation safety act as barriers to diffusion. Expert interpretations for definitional and semantic meanings associated with aviation safety terminology and concepts often vary. The need for industry developed data and text-mining tools used to enhance expert interpretation and development of semantic interpretations related to aviation safety data and information was documented. These tools and processes need to be developed or selected for effectiveness in creating taxonomy and ontology.
4. *Taxonomy and ontology*: The airline industry uses taxonomies and ontologies as a way to reduce semantic ambiguity of aviation safety information within their organizations. Developing taxonomy and ontology was determined essential to managing and diffusing aviation safety information. Variations in expert interpretations and cultural values create challenges to developing taxonomy and ontology. Time and expert resources must be allocated to developing taxonomy and ontology used to disseminate aviation safety information. Developing taxonomy and ontology is highly iterative, and must consider the effect of cultural values on semantic meaning.
5. *Search strategies*: Information overload, complexities related to semantic meaning, cultural differences, and variations in technological standards affect search behavior by stakeholders seeking aviation safety information. U.S. industry

stakeholders prefer to seek information by phone calling, emailing, or talking in-person with colleagues. Personal communication was documented as a way to increase trust and the ability to question validity or meaning applied to data or information within many cultures. Organizations should provide time and access for stakeholders to conduct face-to-face meetings or attend industry conferences related to aviation safety The need for infrastructure enabling search and retrieval processes and strategies for varying forms of data and information useful to the individual was documented. Industry should seek to develop search tools and storage technologies that will enhance retrieval and dissemination of structured and unstructured aviation safety data and information.

6. *Trust, culture, and immunity*: Protecting individuals from public disclosure and retribution or punishment resulting from sharing information was established as essential to sustaining effective aviation information sharing systems. Successful levels of participation in aviation information sharing systems are predicated on strong environments of trust, resulting from the ability to remain anonymous. The ability of aviation safety information sharing systems to provide infrastructure, policies, and laws guaranteeing protection from disclosure is doubted by many industry stakeholders. Therefore, the industry needs to develop and implement ways to manage trust, processes, infrastructure, policies, and laws ensuring confidentiality and immunity from prosecution or liability. These concerns should include (a) minimizing potential negative perception by the public resulting from disclosure, (b) developing agreements and understandings related to trust and confidentiality among varying cultures, (c) presenting cases by trusted

stakeholders demonstrating enhanced cultural values related to the viability of immunity laws or policies, and (d) evaluate and implement strategies and processes for de-identifying and securing collected data.

7. *Learning and feedback*: There are barriers to disseminating aviation safety information and knowledge used to enhance learning. First, it is difficult to track, correlate, and measure the direct impact of shared safety information on aircraft operations and pilot performance. Secondly, the public reacts negatively to proclamations of improved safety, since these statements are often interpreted as an admission of existing safety problems. The importance of creating and diffusing safety bulletins, methods for soliciting feedback, and peer-to-peer mentoring were documented as essential strategies for learning within the aviation industry. However, some organizations and cultures do not have the resources to sustain these types of learning strategies. Therefore, the industry should consider ways to disseminate aviation safety information and knowledge to these organizations or cultures. This concern would include determining and implementing strategies and processes for tracking and disseminating case examples, applications, or best practices resulting from the use of shared aviation safety information. Specific strategies for pilots to provide mentorship and solicit feedback should also be developed and implemented.

8. *Technology and human interaction*: The industry needs to standardize formatting and hardware protocols used to network databases containing aviation safety information. Tools such as software and metadata for using databases should be visible and easy to use. The Web was documented as a preferred infrastructure for

disseminating aviation safety information. Technologies for diffusing aviation safety information should consider designing (a) effective and efficient access, login, navigation, and search and retrieval processes (b) clear descriptions and identifications of types of data or information that can be uploaded or retrieved and (c) features to upload unstructured information or feedback about any relevant topic. Available data and information should be archived, kept open to access, and not moved or deleted.

9. *Networks of practice*: Subjects in this sub-problem were asked to describe barriers to the diffusion of aviation safety information related to global networks of practice. Variations in cultural values and motivations were cited as the most predominate barriers to diffusion within networks of practice. Issues related to variations in standards and information technologies used by members to networks of practice serve as barriers to diffusion. Insufficient knowledge and ability by those charged with implementing and managing networks of practice were also described as a challenges impeding the dissemination of data and information. These individuals are also responsible for developing strategies and tactics for increasing participation by stakeholders to networks of practice. Stakeholders must consider the affects of variations in cultural values, motivations, and technological infrastructure when implementing networks of practice. Strategies for enhancing stakeholder knowledge and abilities related to managing diffusion through networks of practice must also be developed.

10. *Alliance and communities of practice*: Communities of practice comprised of alliances were documented as an effective way to network, negotiate, and solve

issues and barriers related to sharing information within and among companies and other industry stakeholders. Alliances were described as negotiated agreements among stakeholders to share or advocate the sharing of aviation safety information. Individuals within alliances work directly with each other to develop environments of trust, share best practices, and seek new information related to aviation safety. Alliances are more successful when stakeholders are from similar cultures and business operating environments. Therefore, those seeking membership must consider potential barriers and benefits prior to participating within an alliance. Establishing strategies and tactics for implementing alliances and enhancing the diffusion of aviation safety information must be developed. Alliances should also determine ways to act as advocates for the development or support of other alliances.

11. *Alliances and immunity*: Examples of alliances with government agencies were documented as favorable to establishing immunity and maintaining trust within and among aviation safety information sharing systems. Government agencies working with alliances have also assisted in analyzing and solving safety related problems. A potential risk in these types of alliances is that agreements to participate may be improperly used to discover the identity of individuals or organizations involved in regulatory violations. Nevertheless, proper selection of government agencies may help to mitigate breaches to agreements sustaining immunity or confidentiality. For theses reasons, potential benefits and risks associated with government agencies serving as partners to alliances must be evaluated. Internal policies, conditions, and agreements facilitating immunity to

alliance stakeholders must be developed and clearly communicated. Alliances should consider partnering and negotiating agreements, policies, and laws related to immunity with government or legislative agencies.

12. *Networks, databases, and alliances*. Interview subjects suggested the need for a centralized database that could be used to store voluntarily contributed information from other existing aviation safety networks or databases. Various industry alliances would conceptualize and implement the database. Data and information contributed to the database would be de-identified and standardized prior to further diffusion to industry stakeholders.
13. *Legislative Acts*: Industry stakeholders often interpret national legislative Acts related to disclosure and information policy as potential barriers to the diffusion of aviation safety information. These laws and policies usually vary with different cultures. Most cultures will not honor the conditions of other national policies and laws related to immunity or disclosure. For these reasons, stakeholders should remain aware of relevant legislative Acts and evaluate the potential of these laws and policies to affect the diffusion of aviation safety information.

The second hypothesis.

The second hypothesis in this study was that processes within GAIN that may affect the diffusion of airline or aviation safety information can be identified and described by processes generalized to the KM taxonomy. The KM taxonomy created in the first sub-problem was used to build constructs for investigating issues and concerns affecting the diffusion of aviation safety information within and among various communities and networks of practice. The resulting taxonomy and related ontologies interpreted in this sub-problem describe issues and concerns relevant to GAIN as a community and network of practice. Therefore, the taxonomy and related ontology presented in this sub-problem support the second hypothesis for this study.

Strengths, weaknesses, or limitations of the research in the second sub-problem.

Interview data collected for this sub-problem revealed expert knowledge describing issues related to the diffusion of aviation safety information. Specifically, insights were provided regarding the aspects of public disclosure and information policy acting as barriers to the diffusion of aviation safety information. These issues are challenges to GAIN and other similar communities and networks of practice.

The lack of interview data from government representatives with experience related to aviation safety information sharing systems created a deficiency in data needed for adequately analyzing this sub-problem. However, several subjects had considerable experience interacting with government agencies while implementing various aviation safety information sharing programs. Their insights were helpful in assessing issues related to disclosure and information policy from a perspective related to government concerns.

Conclusions of the Third Sub-problem

GAIN is presented within a thematic framework of disclosure, policy, and diffusion within the third sub-problem. This investigator documented GAIN’s working groups as concerns interested in addressing the affects of disclosure and related policies on the diffusion aviation safety information.

Interpretations for this sub-problem were derived from the taxonomy and ontology presented in the second sub-problem. From these interpretations, potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information within GAIN's community and network of practice were interpreted, evaluated, and presented. The following sections summarize those recommendations.

1. *Developing and negotiating policies related to disclosure*: GAIN working groups have investigated and described many issues related to risks associated with disclosure. Seeking access and embracing issues related to disclosure for privately owned or confidential sources requires careful negotiation and collaboration between all stakeholders. In many industries, collaboration and negotiation are key strategies for addressing issues related to public disclosure and are essential to building non-punitive cultures (Graham, 2002). Collaborative environments should employ or retain experts to help solve problems within or among communities of practice (Hildreth, 2004). Information or knowledge experts facilitate participation of stakeholders and often negotiate levels of interaction so that they are aligned with concerns related to disclosure (Wenger, 1998). For these reasons, *GAIN should establish a community of practice that can, (a) assist in negotiating and developing collaborative environments addressing issues related to disclosure within and among various alliances, communities, or networks seeking to share aviation safety information, and (b) offer expertise that*

will help stakeholders evaluate and align disclosure policies with associated risks.

2. *De-identifying data and information*: GAIN's Working Group IV addressed concerns related to the de-identification of aviation safety information held in databases. De-identification is essential to building stakeholder trust. Experts and best practices should be used to protect and retain the value of de-identified data (Gupta, Saul, & Gilbertson, 2004). Organizations concerned with de-identification should evaluate software specifically designed to remove or protect the identity of individuals contained in electronic data files (Hernon, Relyea, Dugan, & Cheverie, 2002). For these reasons, *GAIN should develop a community of practice designed to provide industry stakeholders with expertise, technologies, and best practices useful in the de-identification of data or information.*
3. *Securing data, information, and privacy of communication*: GAIN working groups considered the need for processes and policies applied to securing data, information, and the privacy of communication. Securing data, information, and privacy of networks are primary concerns to facilitating communication (Meadow, 1992). Individuals and entities must evaluate risks and implement strategies for controlling security and privacy related to issues such as hardware, software, systems, applications, and human resources, within and among communities and networks of practice (Jamieson & Handzic, 2003). For these reasons, *GAIN should develop a community of practice providing expertise, technologies, and best practices useful in securing data, information, and the*

privacy of communication within and among aviation safety information sharing systems.

4. *Utilizing information polices and laws related to disclosure*: The GAIN Government Support Team was established to investigate and evaluate information policies and laws that may affect the development of aviation information sharing systems. Legal or statutory concerns related to the diffusion of information have been documented in this study as key barriers to sharing aviation safety information. Marett (2002) suggested that information professionals should be concerned with analyzing and employing information laws and policies for managing the use and misuse of disseminated information. Information sharing environments managing disclosure as a means to reduce risks will require unique architectures of information laws and policies (Graham, 2002). Information brokers or other intermediaries often negotiate considerations concerning disclosure and related information policies (Graham, 2002; Marett). For these reasons*, GAIN should develop a community of practice helping stakeholders analyze, design, and manage varying architectures of information policies and laws related to disclosure.*

5. *Creating environments of trust*: This researcher has documented environments of trust as essential to the success of aviation safety information sharing systems attempting to manage risks from the disclosure of data, information, or knowledge. The First and Second GAIN Conferences identified establishing environments of trust as a key strategy for GAIN as a community and network of practice. Hildreth (2004) described the creation of trust between stakeholders as a

key responsibility of communities of practice. Authors such as Buckowitz and Williams (2000), Ford (2003), and Wenger, McDermott, and Snyder (2002) have provided guidelines, policies, and processes for building environments of trust within and among communities and networks of practice. Within the context of KM and diffusion, Ford presents a taxonomy and ontology of concerns and recommendations for solving issues related to trust. In addition to these tools, building trust also includes the development of non-disclosure policies and contracts (Magg & Flint, 2004) and "contracts of reciprocity" (Buckowitz & Williams, p. 196). For these reasons, and along with the aforementioned rationales and recommendations, *GAIN should become a community of practice dedicated to facilitating environments of trust within and among alliances, communities, or networks seeking to diffuse aviation safety information. A prime goal for GAIN should be to develop and investigate policies and processes for continuously managing trust as related to issues of disclosure within and among aviation safety information sharing systems. GAIN should also assist these stakeholders in developing policies and contracts of fair process or procedural justice addressing issues of risks associated with public disclosure of aviation safety information.*

The third hypothesis.

The hypothesis for the third sub-problem was that processes generalized to KM can elucidate solutions to improve the diffusion of airline or aviation safety information within GAIN's network of practice. The evidence and interpretations made in this sub-problem were developed from taxonomies and ontologies grounded in applied and theoretical foundations of KM. The recommendations made in this sub-problem should be useful to GAIN for facilitating the diffusion of airline or aviation safety information within its network of practice, and within and among other alliances, communities, or networks of practice. Therefore, the conclusions in this analysis support the hypothesis for the third sub-problem.

Strengths, weaknesses, or limitations of the research in the third sub-problem.

A strength of the third sub-problem was the presentation of rationales and recommendations that may improve the diffusion of airline or aviation safety information within GAIN’s network of practice. These recommendations in policy may also be applied to other alliances, communities, or networks desiring to disseminate aviation safety information.

A limitation of this sub-problem was that potential solutions for addressing specific barriers related to public disclosure and unique to individual stakeholders are not presented. Rather, this sub-problem offered generalized policy guidelines that may serve as a starting point to address specific issues related to public disclosure as a barrier to the diffusion of aviation safety information.

The problem investigated in this dissertation was that the identification and evaluation of potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information among various organizations has not been studied. The sub-problems in this study were used to investigate issues and potential solutions related to public disclosure as a barrier to knowledge diffusion within the domains of KM, aviation safety information sharing systems, and GAIN. In these ways, the goals for this dissertation have been accomplished.

Conclusions of the Case Study of GAIN

This dissertation examined GAIN as a case study. The original goal of GAIN was to establish a global network for the dissemination of aviation safety information. Some members of GAIN's leadership had hoped the creation of a global aviation information network would eventually eliminate all aircraft accidents within the global airline industry. At the time of this writing, GAIN had not succeeded in accomplishing these goals. In early 2006, GAIN officially announced that it had lost funding from the FAA, and was seeking recommendations for continuing its capability as an aviation safety related organization (E. Fell, personal communication, February 21, 2006; GAIN, 2006).

In April 2006, the U.S. FAA Flight Standards Service hosted the Shared Vision of Aviation Safety Conference in Denver, Colorado. Conversations between various stakeholders attending the conference and this researcher revealed that some industry members had doubted GAIN's ability to become a global aviation information network. Some attendees attributed GAIN's failure to its inability to develop or implement immunity policies and related legislative Acts protecting individuals that disclose aviation safety information.[34] In this study, issues of trust and immunity from disclosure within and among various information ecologies were identified as key challenges to GAIN's success as a global aviation information network.

---

[34] The U.S. FAA's decision to cease funding for GAIN was described by some individuals attending the conference as politically motivated. Therefore, none of the individuals interviewed at the conference would grant permission to have their identity disclosed in this study.

Conversations at the Shared Vision of Aviation Safety Conference also revealed that GAIN's leadership might not have fully recognized the potential consequences of information overload in efforts to establish a global aviation information network. Subjects in this study described how large amounts of safety information collected within their organizations were difficult to manage and analyze (S_8, S_9). Various attendees at the conference and subjects in this study (S_2, S_3, S_8, S_9) indicated that information overload, along with concerns of public disclosure, have caused many airlines to limit the diffusion of aviation safety information. According to these individuals, many airlines prefer the negotiated dissemination of proprietary aviation safety information, rather than open access to industry stakeholders' centralized databases.

Stakeholders in GAIN hoped that software designed for producing automated ontology and taxonomy would diminish some of the concerns related to information overload. All of the subjects in this study and several attendees at the Shared Vision of Aviation Safety Conference reiterated these tools' usefulness in helping to analyze aviation safety data and information. However, these individuals further explained their preference for human interpretation of data and information in order to obtain greater levels of meaning, knowledge, and wisdom as related to aviation safety.

In follow-up discussions, Subjects S_6 and S_8 indicated their organizations no longer use software for automatically generating ontology and taxonomy. These subjects and Subject S_3 recommended that airlines employ professionals with an understanding of the challenges and processes inherent in interpreting ontology and taxonomy. Subject S_3 emphasized expert interpretation of ontology and taxonomy as the most effective way to reduce cultural bias in semantic meaning derived from aviation safety data and information.

As a case study, GAIN is a primary example of challenges facing organizations desiring to manage and diffuse information across various cultural and technological boundaries. Specifically, GAIN demonstrates important relationships among disclosure, information policies, and knowledge diffusion. These challenges, coupled with a loss of funding, caused GAIN to terminate strategies for serving as a global aviation information network.

This researcher recommends that GAIN should leverage its experiences and knowledge base by evolving into a community of practice serving as an information intermediary. Acting as an intermediary, GAIN should serve alliances seeking to negotiate the sharing of aviation safety information. GAIN should assist with creating environments of trust, collaboration, and policies and fair processes for addressing public disclosure as a barrier to the diffusion of aviation safety information within each alliance.

Implications of the Study

Rayward (1998) states that, “information science deals with something that is now and ever has been fundamental to human society” (p. 15). According to Rayward and Despres and Chauvel (2000b), concerns for managing or controlling the flow of information or knowledge have evolved with global society. This dissertation is a contribution to the domain of information science in that it investigated processes and policies used by various cultures and societies to control and manage the diffusion of information and knowledge. The analyses and interpretations made in this study should be useful to the student or practitioner desiring to investigate the phenomena of knowledge diffusion.

Information science is also a domain for studying or applying processes and policies related to access and disclosure of information and knowledge (Machlup & Mansfield, 1983). As a case study, this work analyzed and made recommendations for managing risks related to disclosure as a barrier to the diffusion of aviation safety information. These results should be helpful to stakeholders in the aviation industry seeking to enhance the dissemination of safety information. Individuals or entities in other settings may also apply the results in cases where public disclosure is a barrier to knowledge diffusion. The results of this study should also enhance the understanding or insights of those interested in conducting additional research investigating disclosure and knowledge diffusion.

KM was described as a domain for managing processes and policies within information environments that control knowledge diffusion (Davenport & Prusak, 2000; Smith & McKeen, 2003a). This investigator developed two new taxonomies with related ontologies characterizing KM. The first taxonomy represents a generalized model of KM. This model may be used to further analyze or discover relationships between KM and knowledge diffusion, or prescribe KM related processes and policies that affect knowledge diffusion. The second taxonomy is grounded in KM and focuses on barriers to the dissemination of aviation safety information. This specialized taxonomy is comprised of issues that should be considered when developing or researching aviation safety information sharing systems within and among communities or networks of practice.

Alliances or communities and networks of practice may use recommendations made in this study to manage risks resulting from the public disclosure of aviation safety information.

As a field of study, information science utilizes interpretative processes and technologies such as content analysis and text processing software to categorize and analyze data and information (Debons & Horne, 1998). Content analysis and text-mining software were used to help interpret and develop the taxonomies, ontologies, and recommendations made in this study. This dissertation presents models for using content analysis and text-mining technologies to develop taxonomy and related ontology from published documentation and recorded interviews. Practitioners may use the methodology of this study to refine or apply strategies for building taxonomy and ontology in other areas of study.

Recommendations of the Study

This dissertation produced a generalized taxonomy and ontology of KM based on evidence from the literature. Interpretations of the taxonomy with related ontology were derived from methods using content analysis and text-mining. The interpretative nature of this work provides opportunity for investigating and interpreting alternative or refined outcomes related to KM taxonomy and ontology. Therefore, the methodologies used in this study to develop the generalized taxonomy and related ontologies of KM should be replicated and further developed.

The generalized taxonomy of KM in this work provides themes or concepts that may be studied individually. Research addressing each of these elements should be conducted to discover new concepts or principles related to KM. Future work should incorporate greater use of interview methodologies to examine and enhance the discovery of new concepts or themes related to KM. A strategy for addressing this recommendation would be to complement the results of this work with investigations of KM applied in a variety of specific domains.

A taxonomy with related ontology was also developed specific to the domain of aviation safety information sharing systems. This taxonomy represents themes or concepts that should be considered when disseminating aviation safety information across boundaries. The methodologies used in this analysis may be applied to the study of information sharing systems in other settings. Those interested in sharing aviation safety information may use this work as a starting point to investigate other types of information sharing systems where public disclosure impedes diffusion. Through these efforts, current and future aviation safety information sharing systems may discover new solutions or policies for addressing disclosure as a barrier to knowledge diffusion.

Summary of the Study

In 1996, the U.S. Federal Aviation Administration initiated the Global Aviation Information Network in response to U.S. Government policies seeking ways to eliminate airline accidents worldwide (Hinson, 1995; Orlady & Orlady, 1999). GAIN's primary mission is to identify, collect, analyze, and share airline safety data, information, or knowledge among stakeholders to the global aviation industry. These efforts require cooperative sharing of information and knowledge across cultural, political, and technological boundaries. Therefore, GAIN's success depends on its ability to interconnect and sustain participation by many cultures, organizations, and individuals. This researcher examined GAIN's ability address these issues in environments where risks of public disclosure act as barriers to the diffusion of aviation safety information.

GAIN is a highly complex, dynamic, and evolving system consisting of stakeholders, processes, policies, and technologies that affect knowledge diffusion. Davenport and Prusak (2000) and Smith and McKeen (2003a) recommended the domain of "knowledge management" as a system of processes and policies used to control knowledge diffusion. Therefore, GAIN was examined in this study as a case of applied KM.

Challenges to the GAIN initiative include developing policies, technologies, and legislation that will reduce barriers to the diffusion of airline safety resulting from risks associated with public disclosure (Hart, 1996). Therefore, the problem investigated in this research was to identify and evaluate potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information among various organizations.

This investigation began with a review of related literature. The literature presents GAIN as a community and network of practice. Discussions from the literature described relationships between GAIN and industry communities and networks of practice concerned with mitigating barriers to sharing airline safety information.

The literature review presented characteristics and settings that helped to define communities of practice and networks of practice within knowledge-based environments. Discussions explored relationships between these concerns and KM. Examples of barriers known to affect knowledge diffusion within and among communities and networks of practice were presented. A brief history of the evolution of KM leading to the advent of the knowledge worker is also included.

A detailed case-based description of the development of GAIN initiatives and policies related to barriers in sharing airline safety information was described in the literature review. These descriptions include discussions related to the impact of public disclosure and various national government information policies and legislation on the GAIN initiative. Reviewed material included other cases related to government-sponsored organizations dedicated to the sharing of aviation or airline safety data, information, and knowledge. In contrast to GAIN, the review presents cases of safety and security information sharing systems for domains such as the medical industry, national security, and business.

Government information policies and related legislation create concern and influence the risk of public disclosure to those reporting to aviation safety sharing systems. Therefore, the literature review emphasized government information policies such as the U.S. Freedom of Information Act and other national initiatives affecting access to information.

Literature described processes of KM influencing the effectiveness of knowledge diffusion. Therefore, known barriers that may impede the implementation of KM were also included. The review concluded with recommendations based on evidence from the literature to examine GAIN as a case study demonstrating the interaction between information policy and KM, and their impact on the diffusion of aviation safety information. Three sub-problems were researched to complete the investigation of these concerns.

The first sub-problem investigated the interaction between KM and knowledge diffusion. The hypothesis for this analysis was that issues related to KM that can directly affect the diffusion of data, information, or knowledge among organizations can be generalized as a taxonomy. A generalized taxonomy and ontology of KM was produced in this sub-problem (see Table 11). This taxonomy represents grounded theory developed from a comprehensive examination of examples and cases of KM contained in the literature. The taxonomy may be used to address challenges related to data, information, or knowledge diffusion in a variety of settings or domains.

The second sub-problem in this study was to create specialized taxonomy addressing issues controlling the diffusion of airline safety information. The hypothesis for this analysis was that processes within GAIN that may affect the diffusion of airline or aviation safety information can be identified and described by processes generalized to the KM taxonomy developed in the first sub-problem. The KM taxonomy created in the first sub-problem was used to build constructs for investigating issues and concerns affecting the diffusion of aviation safety information within and among various communities and networks of practice.

Interview data collected for the second sub-problem revealed expert knowledge describing issues related to the diffusion of aviation safety information. These insights revealed aspects of public disclosure and information policy acting as barriers to the diffusion of aviation safety information. The resulting taxonomy and related ontologies interpreted in this sub-problem described issues and concerns relevant to GAIN as a community and network of practice. The taxonomy presented issues related to diffusion, disclosure, and policy that may be used in the design and implementation of airline safety information sharing systems (see Table 13).

In the final sub-problem, GAIN was presented within a thematic framework of disclosure, policy, and diffusion. The hypothesis for this sub-problem was that processes generalized to KM can elucidate solutions to improve the diffusion of aviation safety information within GAIN's network of practice. The evidence and interpretations made in this sub-problem were developed from taxonomies and ontologies grounded in applied and theoretical foundations of KM developed in the first and second sub-problems. From these interpretations, potential solutions to policy issues in public disclosure that prevent the collection and sharing of aviation safety information within GAIN's community and network of practice were interpreted, evaluated, and presented (see Table 14).

Content analysis and text-mining processes were used to help interpret and develop the taxonomies, ontologies, and recommendations made in this study. This dissertation presents models for using content analysis and text-mining technologies to develop taxonomy and related ontology from published documentation and recorded interviews. Practitioners may use the methodology of this study to refine or apply strategies for building taxonomy and ontology in other areas of study.

This dissertation is a contribution to the domain of information science in that it investigated processes and policies used by various cultures and societies to control and manage knowledge diffusion. The study should be helpful to those seeking to study or enhance the dissemination of information in cases where public disclosure is a barrier to knowledge diffusion.

This dissertation examined GAIN as a case study. Based on the evidence presented from the literature and interpretations and conclusions drawn from this study, it is recommended that GAIN should evolve into a community of practice serving as an information intermediary to various alliances seeking to share aviation safety information. GAIN should focus on assisting alliances with creating environments of trust, collaboration, and the development of policies and fair processes for addressing public disclosure as a barrier to the diffusion of aviation safety information.

Appendix A

Definitions of Knowledge Management from the Literature

(Sorted in Ascending Order of Known Publication Date)

1. "Although there is no single, agreed-upon approach to the practice, knowledge management, in general, encompasses a variety of strategies, methods, and technologies for leveraging the intellectual capital and know-how of organizations for competitive advantage." (Menon & Varadarajan's study, as cited in Barclay & Pinelli, 1997, p. 906)
2. "In practice, knowledge management often encompasses identifying and mapping intellectual assets within the organization, generating new knowledge for competitive advantage within the organization, making vast amounts of corporate information accessible, sharing of best practices, and technology that enables all of the above — including groupware and intranets." (Barclay & Murray, 1997, para. 1)
3. "Knowledge Management isn't a technology, but rather a management concept. It is a way of reorganizing the way knowledge is created, used, shared, and stored in an organization." (Wohl, 1997, p. 1)
4. "Knowledge management is, in part, a recognition of the desperate need for a centripetal, integrative force in business that counteracts the forces of infoglut and technology." (Hanley, 1998, para. 2)
5. "…working with objects (data or information) is Information Management and working with people is Knowledge Management." (Grey, 1998, para. 3)
6. "Definitions of knowledge management vary widely. The term is being applied to products ranging from search engines to call-center software." (Hibbard, 1998, para. 2)
7. "Knowledge management is therefore a conscious strategy of getting the right knowledge to the right people at the right time and helping people share and put information into action in ways that strive to improve organizational performance." (O'Dell & Grayson, 1998, p. 6)

Appendix A *(continued)*

8. Mine is simply this: making sure the knowledge you have within a work group is known to, and available to, others in the organization.” (Lovelace, 1999)
9. “As the industry wrestles to define knowledge management and describe what it includes (or excludes), many have supported the notion that KM is not a technology or set of technologies, but also must comprise an engineered set of processes that facilitate knowledge sharing.” (KMWorld.com., 1999, para. 1)
10. “KM is a newly emerging, interdisciplinary business model dealing with all aspects of knowledge within the context of the firm, including knowledge creation, codification, sharing, and how these activities promote learning and innovation. In practice, KM encompasses both technological tools and organizational routines in overlapping parts.” (Gotcha, 1999, para. 1)
11. “Knowledge Management (KM) is about getting the right knowledge to the right people at the right time through a collection of technologies, tools and philosophies.” (San Diego State University, 1999, para. 1).
12. “Knowledge management is a lens that helps executives focus on what they should be managing.” (W. Bukowitz as interviewed in Glasser, 1999)
13. “Knowledge management is one way that you can connect the dots and create a picture of new ways of generating and sustaining wealth creation.” (R. Williams as interviewed in Glasser, 1999)
14. “Knowledge management--or knowledge sharing, as some of its practitioners prefer to call it--is not about IT; it's about how people share ideas and best practices.” (Chabrow, 1999, para. 1)
15. “Eight of 10 IT executives define knowledge management as a blend of technology and best practices…” (Chabrow, 1999, para. 3)
16. Knowledge management theory is, “An approach to the study of business that attempts to describe the effectiveness of organizations as a function of the efficiency with which they create, store, and apply knowledge to the creation of goods and services.” (Mattison, 1999, p. 23)

Appendix A *(continued)*

17. "KM is the systematic and explicit management of knowledge related activities, practices, programs, and policies within the enterprise." (Wiig, 2000a, p. 6)
18. "KM is information management by another name." (Davenport & Cronin, 2000, KM1)
19. "Km is the management of 'know-how': process and process Ontologies." (Davenport & Cronin, 2000, para. 5)
20. "Knowledge management is a business process, not a technology." (Flash, 2000, para. 7)
21. "Knowledge management is a way of understanding and ordering organizational activity in the interests of organizational viability." (Davenport & Cronin, 2000)
22. "The strategic use of information and knowledge resources to an organization's best advantage." (University of Toronto, 2000)
23. "We refer to the development and leveraging of organizational knowledge to increase a firm's value as knowledge management." (Smith, 2000, p. 303)
24. "Knowledge Management: A) make an organization's knowledge stores more accessible and useful. B) a business activity with two primary aspects: (1) treating the knowledge component of business activities as an explicit concern of business reflected in strategy, policy, and practice at all levels of the organization and (2) making a direct connection between an organization's intellectual assets — both explicit [recorded] and tacit [personal know-how] — and positive business results. (3) conscious strategy of getting the right knowledge to the right people at the right time and helping people share and put information into action in ways that strive to improve organizational performance." (International Center for Applied Studies in Information Technology, 2001)
25. "Knowledge management is a tool set for the automation of deductive or inherent relationships between information objects, users, and processes." (Frappaolo & Toms' paper, as cited in Fourth Wave Group, 2001)
26. Knowledge management is, "The systematic process of finding, selecting, organizing, distilling, and presenting information in a way that improves an employee's comprehension in a specific area of interest." (University of Texas, 2001)

Appendix A *(continued)*

27. "Knowledge Management practice can be broadly defined as the acquisition, sharing, and use of knowledge within organizations, including learning processes and management information systems." (Warwick University, Business Processes Resource Centre, 2001)

28. "Knowledge management is an ambiguous and inconsistently used term that refers to a broad category of business practices and related technology "tools" that may be associated with the cultivation and business application of intellectual capital (IC). By our preferred, compact definition, knowledge management is any activity that enhances the enterprise's stock of intellectual capital." (Fourth Wave Group, 2001, para. 1)

29. "Even the experts do not have a ready and widely accepted definition of what KM really is. Knowledge management is still seen to be in a phase of self-discovery. We can better describe what it is not by using sentences such as 'Knowledge is more than just information or data'." (Dueck, 2001, para. 1)

30. It seems to have something to do with growing and harvesting insubstantial stuff such as ideas, practices, and information. It seems to have something to do with groups and communities, not individuals. It seems to have something to do with organizations acting smarter." (Weinberger, 2001, para. 7)

31. "Knowledge management … is the name given to the set of systematic and disciplined actions that an organization can take to obtain the greatest value from the knowledge available to it." (Marwick, 2001, para. 2)

32. "Knowledge Management caters to the critical issues of organizational adaption [sic], survival, and competence in face of increasingly discontinuous environmental change.... Essentially, it embodies organizational processes that seek synergistic combination of data and information processing capacity of information technologies, and the creative and innovative capacity of human beings." (Malhotra, 2001, p. 47)

33. "Knowledge management is a key component of collaboration." (Foley, 2001, para. 2)

34. "Knowledge management is the process of transforming information and intellectual assets into enduring value." (Kidwell, Linde, & Johnson, 2000, p. 3)

Appendix A *(continued)*

35. "Knowledge management, which includes retrieval, storage, discovery, and capture of knowledge, aims to facilitate the flow of information across an enterprise. The concept transcends technology, having a broader emphasis on services and methods to boost acceptance of new processes within the corporate culture, training and learning services, collaboration, and security." ("Information and Command and Control," 2001, p. 48)
36. "By definition, … most knowledge management work is concerned with groups, communities, and networks." (Prusak, 2001, p. 1006)
37. "we have seen a tendency – especially among vendors of software – to reductively define knowledge management as moving data and documents around" (Prusak, 2001, p. 1003)
38. "KM is a LINUX of management concepts. A 'Movement' of people round the globe connected and contactable via the Net." (Sveiby, 2001,para. 11)
39. "Knowledge management is knowing what we know, capturing and organizing it, and using it to produce returns." (Stewart, 2001, p. 112)
40. "Knowledge management generally describes the use of technology to help an organization understand what information is in their databases and how to find it." (Caterinicchia, 2001, para. 3)
41. "The comprehensive management of the expertise in an organization. It involves collecting, categorizing and disseminating knowledge." (Turban, McLean, & Wetherbe, 2002, p. G-6)
42. "Knowledge management is the discipline dedicated to more deliberate means of people creating and sharing knowledge - data, information, and understanding in a social context - to make the right decisions and take the right actions." (KM.Gov, 2002, para. 1)
43. "Knowledge Management is the ability to create and transfer as much of the right knowledge as possible to support as many people as possible in the best method possible in order to have a positive impact on the business. It's about bringing the full weight of the company's knowledge base (hardware, software, and people) to bear, in a relevant and useful manner, upon the requirements of the user; thus enabling the individual and the organization to learn and adapt." (Friedman, 2002)

Appendix A *(continued)*

44. "KM can be defined as an effort to make accessible and share not only explicit factual information but also the tacit knowledge that exists in an organization in order to advance the organization's mission." (McInerney, 2002, para. 1)
45. "… any process or practice of creating, acquiring, capturing, sharing and using knowledge, wherever it resides, to enhance learning and performance in organizations." (Swan, Scarbrough, & Preston's paper, as cited in *CiteSteer*, 2002, para. 1)
46. "KM is a management discipline that focuses on enhancing knowledge production and integration in organizations." (McElroy, 2003, p. 216)
47. "Knowledge processing is a set of social processes through which people in organizations create and integrate their knowledge. Knowledge management is a management activity that seeks to enhance knowledge processing." (McElroy, 2003, p. 54)
48. KM is a strategy for helping entities to increase their "capacity to learn, innovate, and adapt change." (McElroy, 2003, p. 69)
49. "knowledge management is all about sustainable innovation." (McElroy, 2003, p. 103)
50. "In other words, if KM is the answer, what was the question?" (McElroy, 2003, p. 84)
51. "Knowledge management is 95% people politics, processes and culture and 5% technology." (Tom Peters, as cited in Auditore, 2003)
52. "But at its core, KM is the process through which an enterprise uses its collective intelligence to accomplish its strategic objectives." (Barquin, 2003, p. 5)
53. "'The New Knowledge Management' (TNKM) is the name for a body of issues, models, and practices representing the broadening of scope of knowledge management from a concern with knowledge sharing, broadcasting, retrieval, and teaching, collectively *knowledge integration*, to a concern with these things, as well as *knowledge making*, or *knowledge production*. (Firestone & McElroy, 2004, p. xix)
54. "KM is the extension , broadly across the firm, of the information environment that has been shown by research to be conductive to successful R&D." (Koenig, 2004, p. 113)

Appendix B

Number of Organizations by Category Attending the First Global Analysis and Information Network Conference, October 1996, Boston

Category	Number	Percentage
Airlines	8	9%
U.S.	*5*	*6%*
Non-U.S.	*3*	*3%*
Aviation Trade Associations	8	9%
Consulting Organizations or Individuals Involved in Consulting, All Categories	34	39%
Aviation	*22*	*25%*
Information Technology	*9*	*10%*
Federally Funded Research & Development Centers	*2*	*2%*
Other	*1*	*1%*
Government Organizations	19	22%
Civil Aviation Authorities	*4*	*5%*
Accident Investigation Boards	*2*	*2%*
Research Groups	*5*	*6%*
Military Aviators	*5*	*6%*
Confidential Reporting Programs	*1*	*1%*

Appendix B *(continued)*

Category	Number	Percentage
Other	*2*	*2%*
Insurance	1	1%
Manufacturers of Aviation Products	9	10%
Media	2	2%
Other / Not Classified	2	2%
Universities	5	6%
Total	**88**	**100%**

Note. From the "Conference Participant Profiles" (GAIN, 2002c).

Percentages rounded to nearest whole number.

A total of 153 individuals attended this conference.

Appendix C

Obstacles and Potential Solutions to GAIN as Identified at the First Global Analysis and Information Network Conference, October 1996, Boston

Category	**Potential Solution(s)**
Litigation / Liability / Regulation	Amend the laws
	De-identify sources
	Locate GAIN offshore (out of the U.S.)
	Consider excluding countries where safety information cannot be protected
	ICAO could exert pressure on countries to protect safety information
Financial Support Potential Solutions	U.S. Government-FAA grant
	Member dues
	U.N./ICAO Funding
	Corporate R&D (Speculative funding / public relations funding)
	Venture capital
	Aviation insurers
	Self-funding (through service fees)

Appendix C *(continued)*

Category	**Potential Solution(s)**
Human Factors (HF) data is not hard data / pilots' perceptions unknown	Potential Solutions: APMS / Video / CVR Data Applied thru GAIN Pilot Surveys Structured Call-Backs
No off-duty data	Dupont's approach to encourage self and team disclosure
Lack of fatigue and aeromedical data on pilots and crew	A personal pre-flight check list that can be analyzed ("I'm okay" checklist results)
Air traffic controller and pilot communications issues	CVR / APMS / ATC radar data shown side by side (time synchronized) and then analyzed
Different terminology & approaches applied to human factors analysis	Using more data with automated tools will encourage standardized human factors analysis
Security	Encryption Different levels of access Data administrator Back-up data Virus scan

Appendix C *(continued)*

Category	Potential Solution(s)
Data Collection & Standardization	Focus groups that develop solutions to specific problems
	Expert system/artificial intelligence developed and applied to data analysis
	Users agree to protect information at the same level in which it is received to get access to the system
	Develop protocols to enforce standards
	Secure intranet warehouse to a central data base so data is available for analysis in its original form
Data Analysis & Dissemination	Perform analysis across several systems to verify validity of safety issues
	Conduct pilot projects to test analysis methods
	Start small and work out the issues
	Manufacturers receive information from carriers, analyze the information, provide results to GAIN, and thereby maintain security of source
	Learn from organizations with analytical skills

Appendix C *(continued)*

Category	**Potential Solution(s)**
Leadership & Coordination	Give leadership to ICAO
	Give leadership to Flight Safety Foundation
	Create new membership organization to operate GAIN
	Share leadership
	Provide legal immunity for leader to encourage a party to assume that role
	Encourage broad-based leadership
	Let the market decide leadership
Trust	Enforceable code of conduct to which everyone agrees
	Legal nondisclosure agreements
	Establish agreed-to-in-advance penalties for infractions
	Build working relationships among the participants

Appendix D

Number of Organizations by Category Attending the Second Global Analysis and Information Network Conference, May 1997, London

Category	Number	Percentage
Airlines	17	15%
U.S.	*3*	*3%*
Non-U.S.	*14*	*12%*
Aviation Trade Associations	11	10%
Consulting Organizations or Individuals Involved in Consulting, All Categories	18	16%
Aviation	*16*	*14%*
Information Technology	*1*	*1%*
Federally Funded Research & Development Centers	*1*	*1%*
Other	*0*	*0%*
Government Organizations	36	31%
Civil Aviation Authorities	*15*	*13%*
Accident Investigation Boards	*4*	*3%*
Research Groups	*3*	*3%*
Military Aviators	*2*	*2%*
Confidential Reporting Programs	*5*	*4%*

Appendix D *(continued)*

Category	Number	Percentage
Other	*7*	*6%*
Insurance	2	2%
Manufacturers of Aviation Products	18	16%
Media	3	3%
Other / Not Classified	4	3%
Universities	6	5%
Total	**115**	**100%**

Note. From the “Conference Participant Profiles” (GAIN, 2002c).

Percentages rounded to nearest whole number.

A total of 166 individuals attended this conference.

Appendix E

Number of Organizations by Category Attending the Third Global Analysis and Information Network Conference, November 1998, Long Beach

Category	Number	Percentage
Airlines	33	27%
U.S.	*16*	*13%*
Non-U.S.	*17*	*14%*
Aviation Trade Associations	14	11%
Consulting Organizations or Individuals Involved in Consulting, All Categories	19	15%
Aviation	*16*	*13%*
Information Technology	*1*	*1%*
Federally Funded Research & Development Centers	*2*	*2%*
Other	*0*	0%
Government Organizations	33	27%
Civil Aviation Authorities	*11*	*9%*
Accident Investigation Boards	*4*	*3%*
Research Groups	*6*	*5%*
Military Aviators	*4*	*3%*
Confidential Reporting Programs	*3*	*2%*

Appendix E *(continued)*

Category	**Number**	**Percentage**
Other	*5*	*4%*
Insurance	1	1%
Manufacturers of Aviation Products	13	10%
Media	4	3%
Other / Not Classified	4	3%
Universities	3	2%
Total	**269**	**100%**

Note. From the "Conference Participant Profiles" (GAIN, 2002c).

Percentages rounded to nearest whole number.

A total of 195 individuals attended this conference.

Appendix F

Number of Organizations by Category Attending the Fourth Global Analysis and Information Network Conference, June 2000, Paris

Category	Number	Percentage
Airlines	29	28%
U.S.	*4*	*4%*
Non-U.S.	*25*	*25%*
Aviation Trade Associations	8	8%
Consulting Organizations or Individuals Involved in Consulting, All Categories	18	18%
Aviation	*17*	*17%*
Information Technology	*0*	*0%*
Federally Funded Research & Development Centers	*1*	*1%*
Other	*0*	*0%*
Government Organizations	22	22%
Civil Aviation Authorities	*12*	*12%*
Accident Investigation Boards	*1*	*1%*
Research Groups	*2*	*2%*
Military Aviators	*1*	*1%*
Confidential Reporting Programs	*1*	*1%*

Appendix F *(continued)*

Category	**Number**	**Percentage**
Other	*5*	*5%*
Insurance	3	3%
Manufacturers of Aviation Products	12	12%
Media	0	0%
Other / Not Classified	6	6%
Universities	4	4%
Total	**102**	**100%**

Note. From the “Conference Participant Profiles” (GAIN, 2002c).

Percentages rounded to nearest whole number.

A total of 179 individuals attended this conference.

Appendix G

Number of Organizations by Category Attending the Fifth Global Analysis and Information Network Conference, December 2001, Miami

Category	Number	Percentage
Airlines	26	15%
U.S.	*13*	*8%*
Non-U.S.	*13*	*8%*
Aviation Trade Associations	7	4%
Consulting Organizations or Individuals Involved in Consulting, All Categories	18	10%
Aviation	*15*	*9%*
Information Technology	*0*	*0%*
Federally Funded Research & Development Centers	*0*	*0%*
Other	*3*	*2%*
Government Organizations	23	13%
Civil Aviation Authorities	*11*	*6%*
Accident Investigation Boards	*3*	*2%*
Research Groups	*4*	*2%*
Military Aviators	*3*	*2%*
Confidential Reporting Programs	*0*	*0%*

Appendix G *(continued)*

Category	Number	Percentage
Other	*2*	*1%*
Insurance	1	1%
Manufacturers of Aviation Products	16	9%
Media	1	1%
Other / Not Classified	0%	0%
Universities	4	2%
Total	**96**	**100%**

Note. From the "Conference Participant Profiles" (GAIN, 2002c).

Percentages rounded to nearest whole number.

A total of 173 individuals attended this conference.

Appendix H

Classifications of Civil Aircraft Accident Information Requests Made through FOIA that are Commonly Denied by the NTSB

The Safety Board denies a FOIA request, completely or in part, only if it falls under one of nine statutory exemptions of FOIA. The four most common exemptions under which the Board withholds information are as follows:

1. Draft reports & staff analysis.

2. Personal information, where a personal interest in privacy outweighs a public interest in release, this includes graphic photographs of injuries in accidents and autopsy reports.

Trade Secrets and/or confidential financial/commercial information submitted by private persons or corporations to the NTSB in the course of an investigation.

1. Information protected from release by another statute. Examples include:

    a. Cockpit Voice Recorder (CVR) tapes. Release of the tapes is prohibited by 49 U.S.C 1114(c). However, the Board will release a CVR transcript [edited or unedited], the timing of such release is also controlled by statute - 49 U.S.C 1114(c)(B);

    b. Voluntarily provided safety-related information. 49 U.S.C 1114(b)(3) prohibits the release of such information if it is not related to the exercise of the Board's accident or incident investigation authority and if the Board finds that the disclosure would inhibit the provision of that type of information; and;

    c. Records or information relating to the NTSB's participation in foreign aircraft accident investigations. 49 U.S.C 1114(e) prohibits the release of this information before the country conducting the investigation releases its report or two years following the accident, whichever occurs first.

Note. From “Answers to Frequently Asked Questions about FOIA” (U.S. National Transportation Safety Board, 2002).

Appendix I

Government and Non-government Agencies Serving as Members to the GAIN Government Support Team (GST) - Fifth GAIN World Conference

GST Government and Non-government GST Members
1. France: Directorate-General of the Civil Aviation (DGAC) and BEA Systems
2. U.K.: Civil Aviation Authority (CAA) and Air Accident Investigations Branch (AAIB)
3. European Commission
4. European Joint Aviation Authorities (JAA)
5. Nordic Group
6. Canada: Transport Canada (TC) and Transportation Safety Board (TSB)
7. Australia: Civil Aviation Safety Authority (CASA) and Australian Transport Safety Bureau (ATSB)
8. Japan: Civil Aviation Bureau of Japan (JCAB)
9. New Zealand: Civil Aviation Authority (CAA) and Transport Accident Investigation Commission (TAIC)
10. U.S.: Federal Aviation Administration (FAA) and National Transportation Safety Board (NTSB)
11. International Civil Aviation Organization (ICAO)

Note. From "Legal Impediments to Safety Information Collection and Sharing." Retrieved July 20, 2002, from http://www.ntsb.gov/info/foia.htm

Appendix J

Key Features and Technological Aspects of *TextAnalyst v2.1*[35]

TextAnalyst is an off-the-shelf text-mining software application designed to provide automatic semantic and classification processing of one or more unstructured natural language text data files (.txt or rtf.). Text-mining software uses proprietary “black box” (Delmater & Hancock, 2001, p. 216) neural network algorithms designed to produce semantic structures of “concepts” inherent to text data files. Neural network applications utilize neuron-like processing units for classifying concepts and determining weighted connections between concepts (Han & Kamber, 2001). A concept identified by *TextAnalyst* may be a single word or represented as a string of words. Concepts within *TextAnalyst* are hyperlinked to their occurrence in text and represented graphically in parent-child “semantic tree structures” (Megaputer, 2003, p. 26).

Semantic tree structures generated by *TextAnalyst* present the relative importance of concepts to each other (nodes) and to the document(s) analyzed. Algorithms evaluate the frequency and relationship of each concept to derive the relative importance or “semantic weight” for each concept identified.

---

[35] *TextAnalyst* is a trademark of Microsystems, LTD. At the time of this writing, Megaputer Intelligence, Inc. maintained exclusive distribution rights for *TextAnalyst.*

Appendix J *(continued)*

Semantic weight in *TextAnalyst* is defined by Megaputer "as the measure of the probability that a concept is contextually important" (2003, p. 26). Semantic weight varies from 0 to 100, with 100 indicating the highest relative importance to either the parent concept or data file(s). Relative importance is indicated by a pair of semantic weights (*x*, *y*) presented adjacent to each concept. The first semantic weight, *x*, indicates the concept's semantic weight in relation to its parent concept. Value y is the semantic weight of a concept to the entire text data file(s) analyzed (Megaputer).

Once *TextAnalyst* has completed semantic analysis, various tools for text-mining may be applied to the results. Megaputer (2003, p. 10) provided the following descriptions for each data-mining tool included in *TextAnalyst*:

- Navigation: *TextAnalyst* hyperlinks key concepts in text to concepts presented in the semantic analyses.
- Summarization: This is a semantically weighted summary containing the most important sentences in the data set. A user defined semantic threshold allows filtering of sentences considered less relevant.
- Natural language queries: Semantically weighted searches are formulated by typing a question in conventional written English.
- Knowledge base development: *TextAnalyst* saves a knowledge base containing data files, semantic network, edits, results of analyses, hyperlinks, and any related dictionaries.
- Topic structure organization: The semantic network displays concepts presented in a topic organization structure. Topic structures include only the most important concepts and clusters them in a nested tree-like structure.
- Dictionary development: *TextAnalyst* provides for the use of default or customized dictionaries. Dictionaries permit the addition of user words, and allow rules adjusting the importance of each of those words.

Appendix J *(continued)*

TextAnalyst is designed to process data for semantic and classification text-mining automatically. *WordNet* is the default dictionary used within *TextAnalyst* to provide a base classification scheme for automatically analyzing natural language text files.[36] Dictionary classification schemes used in text-mining applications use previously classified documents as training sets. Analyzed results using the previously classified documents translate into a classification theme used in the form of "universal" or default dictionaries (Weiss et al., 1999, p. 3).

Default dictionaries are edited by the user in order to improve accuracy or relatedness in the results generated through semantic analysis (Megaputer, 2003; Weiss et al., 1999). The default dictionary in *TextAnalyst* may be edited and saved under a different file name. Megaputer (p. 57) defined the following functions for editing the default dictionary:

- User words (thematic words): specified concepts or themes to be included in the semantic network, regardless if *TextAnalyst* determines them semantically important.
- Dependent words: words considered synonymous to user words. For example, learning may be specified as a user word with training specified as dependent to learning. TextAnalyst automatically replaces dependent words with the specified user word.
- Common words: words considered to have little semantic importance. Examples include adjectives and words the user determines should not be valued semantically as independent concepts. *TextAnalyst* will semantically value common words when they occur with other words producing important semantic concepts.

---

[36] *WordNet* is a lexical database of the English language developed and validated by the Cognitive Science Laboratory at Princeton University (see: http://www.cogsci.priceton.edu/~wn/index.shtml).

Appendix J *(continued)*

- Not analyzed words (deleted words): words or articles the user determines *TextAnalyst* should ignore, regardless of semantic importance.
- Exception words: The user may indicate words that do not follow the usual rules of stemming, such as irregular verb forms.

Appendix K

NOVA Institutional Review Board (IRB) Approval

From: James Cannady [mailto:j.cannady@computer.org]
Sent: Thursday, January 15, 2004 6:23 PM
To: forrestj@nova.edu
Subject: IRB Approval

Jeffrey,

After reviewing your IRB Submission Form and Research Protocol I have approved your proposed research for IRB purposes. Your research has been determined to be exempt from further IRB review based on the following conclusion:

> Research using survey procedures or interview procedures where subjects' identities are thoroughly protected and their answers do not subject them to criminal and civil liability.

Please note that while your research has been approved, additional IRB reviews of your research will be required if any of the following circumstances occur:

1. If you, during the course of conducting your research, revise the research protocol (e.g., making changes to the informed consent form, survey instruments used, or number and nature of subjects).

2. If the portion of your research involving human subjects exceeds 12 months in duration.

Please feel free to contact me in the future if you have any questions regarding my evaluation of your research or the IRB process.

Dr. Cannady

James Cannady, Ph.D.
Assistant Professor

Appendix K *(continued)*

Graduate School of Computer
and Information Sciences
Nova Southeastern University

954.262.2085
404.312.2374 (mobile phone)
cannady@nova.edu

PGP public key fingerprint:
8169 6D03 680E EF6C 899C
8C42 B4A3 DC9F 9F6B 4075

Appendix L

Documents Admitted as Data for the Treatment of the First Sub-problem

(Listed in Descending Order by Year Published)

In Press

Berdrow, I., & Lane, H. W. (in press). International joint ventures: Creating value through successful knowledge management. *Journal of World Business*.

Nielsen, B. B. (in press). The role of knowledge embeddedness in the creation of synergies in strategic alliances. *Journal of Business Research*.

Revilla, E., Sarkis, J., & Acosta, J. (in press). Towards a knowledge management and learning taxonomy for research joint ventures. *Technovation*.

Teo, T. S. H. (in press). Meeting the challenges of knowledge management at the Housing and Development Board. *Decision Support Systems.*

2004

Awazua, Y., & Desouzab, K. C. (2004). The Knowledge Chiefs: CKOs, CLOs and CPOs. *European Management Journal*, *22*(3), 339-344.

Carmen Camelo-Ordaz, M. C., Fernández-Alles, M., Martín-Alcázar, F., Romero-Fernández, P. M., & Valle-Cabrera, R. (2004). Internal diversification strategies and the processes of knowledge creation. *Journal of Knowledge Management, 8*(1), 77-93.

Chuang, S.-H. (2004). A resource-based perspective on knowledge management capability and competitive advantage: An empirical investigation. *Expert Systems with Applications*, *27*(3), 459-465.

Currie, G., & Kerrin, M. (2004). The limits of a technological fix to knowledge management. *Management Learning, 35*(1), 9-29.

Appendix L *(continued)*

Evaristo, J. R., Scudder, R., Desouza, K. C., & Sato, O. (2004). A dimensional analysis of geographically distributed project teams: A case study. *Journal of Engineering and Technology Management*, *21*(3), 175-189.

Ferrari, F. M., & Carlos de Toledo, J. (2004). Analyzing the knowledge management through the product development process. *Journal of Knowledge Management*, *8*(1), 117-129.

Gertler, M. S., & Wolfe, D. A. (2004). Local social knowledge management: Community actors, institutions and multilevel governance in regional foresight exercises. *Futures*, *36*(1), 45-65.

Leseure, M. J., & Brookes, N. J. (2004). Knowledge management benchmarks for project management. *Journal of Knowledge Management*, *8*(1), 103-116.

Möller, K., & Svahn, S. (2004). Crossing East-West boundaries: Knowledge sharing in intercultural business networks. *Industrial Marketing Management*, *33*(3), 219-228.

Takahashi, T., & Vandenbrink, D. (2004). Formative knowledge: From knowledge dichotomy to knowledge geography - knowledge management transformed by the ubiquitous information society. *Journal of Knowledge Management*, *8*(1), 64-76.

2003

Ardichvili, A., Page, V., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management*, *7*(1), 64-77.

Barquin, R. C., Bennet, A., & Remez, S. G. (2003). Conclusion. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 503-505). Vienna, VA: Management Concepts.

Appendix L *(continued)*

Barquin, R. C., Bennet, A., & Remez, S. G. (2003).The GSA story: Swimming with the dolphins. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 453-468). Vienna, VA: Management Concepts.

Bennet, A., & Porter, D. (2003). The force of knowledge, a case study of KM implementation in the Department of the Navy. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 467-487). New York: Springer.

Beveren, J. V. (2003). Does health care for knowledge management. *Journal of Knowledge Management*, *7*(1), 90-95.

Bresnen, M., Edelman, L., Newell, S., Scarbrough, H., & Swan, J. (2003). Social practices and the management of knowledge in project environments. *International Journal of Project Management*, *21*(3), 157-166.

Choi, B., & Lee, H. (2003). An empirical investigation of KM styles and their effect on corporate performance. *Information & Management, 40*(5), 403-417.

Christensen, C. H., & Bang, H. K. (2003). Knowledge management in a project oriented organization: Three perspectives. *Journal of Knowledge Management, 7*(3), 116-128.

Conway, S. (2003). Building a KM foundation at Microsoft Consulting Services. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 565-576). New York: Springer.

Desouza, K. C. (2003). Knowledge management barriers: Why the technology imperative seldom works. *Business Horizons, 46*(1), 25-29.

Desouza, K., & Evaristo, R. (2003). Global knowledge management strategies. *European Management Journal*, *21*(1), 62-67.

DeTore, A. W., & Balliet-Milholland, J. M. (2003). Transforming theory into fact: Hands-on knowledge management initiatives built on a Reinsurer's pile of junk. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 533-547). New York: Springer.

Appendix L *(continued)*

Dried, S. L. (2003). From inventions management to intellectual capital management at the Dow Chemical Company: A 100+ year journey. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 489-500). New York: Springer.

Gabbay, J., le May, A., Jefferson, H., Webb, D., Lovelock, R., Powell, J., & Lathlean, J. (2003). A case study of knowledge management in multi-agency consumer-informed 'communities of practice': Implications for evidence based policy development in health and social service. *Health, 7*(3). 283–310.

Gloet, M., & Berrell, M. (2003). The dual paradigm nature of knowledge management: Implications for achieving quality outcomes in human resource management. *Journal of Knowledge Management, 7*(1), 78-89.

Gottschalk, P., & Khandelwal, V. K. (2003). Determinants of knowledge management technology projects in Australian law firms. *Journal of Knowledge Management, 7*(4), 92-105.

Herder, P. M., Veeneman, W. W., Buitenhuis, M. D. J., & Schaller, A. (2003). Follow the rainbow: A knowledge management framework for new product introduction. *Journal of Knowledge Management, 7*(3), 105-115.

Jermola, M., Lavrač, N., & Urbančič, T. (2003). Managing business intelligence in a virtual enterprise: A case study and knowledge management lessons learned. *Journal of Intelligent & Fuzzy Systems, 14*, 121–136.

Kalling, T. (2003). Knowledge management and the occasional links with performance. *Journal of Knowledge Management, 7*(3), 67-81.

Kelly, T. M., & Bauer, D. K. (2003). Managing intellectual capital - via E-Learning - at Cisco. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 511-532). New York: Springer.

Mason, D., & Pauleen, D. (2003). Perceptions of knowledge management: A qualitative analysis. *Journal of Knowledge Management, 7*(4), 38-48.

Moffett, S., McAdam, R., & Parkinson, S. (2003). An empirical analysis of knowledge management applications. *Journal of Knowledge Management, 7*(3), 6-26.

Appendix L *(continued)*

Murty, K. S. [2003]. Role of HR in institutionalizing knowledge management in a company. *Association of Knowlegework*. Retrieved October 25, 2003 from http://www.kwork.org/White%20Papers/hr-km.html

Nissen, M. E. (2003). Knowledge flow through a military joint task force operation. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 549-563). New York: Springer.

O'Dell, C., Hasanali, F., Hubert, C., Lopez, K., Odem, P., & Raybourn, C. (2003). Successful KM implementations: A study of best-practice organizations. . In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 411-441). New York: Springer.

Pan, S. L., & Leidner, D. E. (2003). Bridging communities of practice with information technology in pursuit of global knowledge sharing. *The Journal of Strategic Information Systems, 12*(1), 71-88.

Roth, J. (2003). Enabling knowledge creation: Learning from an R&D organization. *Journal of Knowledge Management, 7*(1), 32-48.

Salisbury, M. W. (2003). Putting theory into practice to build knowledge management systems. *Journal of Knowledge Management, 7*(2), 128-141.

Schrimer, A. L. (2003). Privacy and knowledge management: Challenges in the design of the Lotus Discovery Server. *IBM Systems Journal, 42*(3), 51-53.

Smith, H. A., & McKeen, J. D. (2003). Knowledge management in organizations: The state of current practice. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 395-410). New York: Springer.

Spring, M. (2003). Knowledge management in extended operations networks. *Journal of Knowledge Management, 7*(3), 29-37.

van der Spek, R., Hofer-Alfeisa, J., & Kingma, J. (2003). The knowledge strategy process. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 443-466). New York: Springer.

Appendix L *(continued)*

Wagner, B. A. (2003). Learning and knowledge transfer in partnering: An empirical case study. *Journal of Knowledge Management*, *7*(2), 97-113.

Wolford, D., & Kwiecien, S. (2003). Driving knowledge management at Ford Motor Company. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 501-510). New York: Springer.

2002

Abou-Zeid, E.-S. (2002). A knowledge management reference model. *Journal of Knowledge Management*, *6*(5), 486-499.

Asleena, H. (2002, October). Knowledge management via IT and business strategies alignment: B2B MSC Companies in Kuala Lumpur, Malaysia. *Journal of Knowledge Management Practice*. Retrieved January 28, 2004 from http://www.tlainc.com/

Burk, M. (2002). Federal Highway Administration knowledge sharing success story: Rumble strips government-to-government community of practice. *The Journal of the Knowledge and Innovation Management Professional Society*, *1*(1). Retrieved January 4, 2004 from http://www.kmpro.org/journal/Vol1_No1_Dec02/industry_focus.cfm

Cinquegrani, R. (2002). Futurist networks: Cases of epistemic community? *Futures*, *34*(8), 779-783.

Contractor, F. J., & Ral, W. (2002). How knowledge attributes influence alliance governance choices. *Journal of International Management*, *8*(1), 11-27.

Dayasindhu, N. (2002). Embeddedness, knowledge transfer, industry clusters and global competitiveness: A case study of the Indian software industry. *Technovation*, *22*(9), 551-560.

Denning, S. (2003). Knowledge sharing at the World Bank. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 469-484). Vienna, VA: Management Concepts.

Appendix L *(continued)*

Dilnutt, R. (2002). Knowledge management in practice: Three contemporary case studies. *International Journal of Accounting Information Systems, 3*(2), 75-81.

Fang, S., Hong, K., Bock, G. W., & Kim, I. (2002). Knowledge management and process innovation: The knowledge transformation path in Samsung SDI. *Journal of Knowledge Management, 6*(5), 479-485.

Fioa, L. A. (2002). Assessing unqualified in-service teacher training in Brazil using knowledge management theory: A case study. *Journal of Knowledge Management, 6*(1), 74-86.

Franz, M., Freudenthaler, K., Kameny, M., & Schoen, S. (2002). The development of the Siemens Knowledge Community Support. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 147-159). New York: Springer.

Franz, M., Schmidt, R., & Seufert, S. (2002). KECnetworking – knowledge management at Infineon Technologies AG. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 128-146). New York: Springer.

Gibbert, M., Jenzowsky, S., Jonczyk, C., Thiel, M., & Völpel, S. (2002). ShareNet - the next generation: Knowledge management. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 42-59). New York: Springer.

Gibbert, M., & Krause, H. (2002). Practice exchange in a best practice marketplace. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 89-107). New York: Springer.

Hariharan, A. (2002, December). Knowledge management: A strategic tool. *Journal of Knowledge Management Practice.* Retrieve January 21, 2004 from http://www.tlainc.com/articl46.htm

Holsapple, C. W., & Joshi, K. D. (2002). Knowledge manipulation activities: Results of a Delphi study. *Information & Management, 39*(6), 477-490.

Appendix L *(continued)*

Igonor, A. (2002, June). Success factors for development of knowledge management in e-Learning in Gulf Region institutions. *Journal of Knowledge Management Practice.* Retrieve January 21, 2004 from http://www.tlainc.com/artic37.htm

Ladd, A., & Ward, M. A. (2002, August). An investigation of environmental factors influencing knowledge transfer. *Journal of Knowledge Management Practice*. Retrieved January 28, 2004 from http://www.tlainc.com/

Lasky, B., & Tare, M. (2002). Knowledge management: A 21st century role for the human resource professional (Swinburne University of Technology). Paper presented at the meeting of IFSAM 2002 Conference, Gold Coast, Queensland, Australia. Retrieved January 26, 2005 from http://www.ifsam.org/2002/Lasky&Tare.pdf

Mudambi, R. (2002). Knowledge management in multinational firms. *Journal of International Management, 8*(1), 1-9.

Na Ubon, A., & Kimble, C. (2002) Knowledge management in online distance education. *Proceedings of the 3rd International Conference on Asynchronous Learning Networks 2002, University of Sheffield, UK, March*, 465-473.

Peña, I. (2002). Knowledge networks as part of an integrated knowledge management approach. *Journal of Knowledge Management, 6*(5), 469-478.

Robertson, S. (2002). A tale of two knowledge-sharing systems. *Journal of Knowledge Management*, *6*(3), 295-308.

Santosus, M. (2002, September). Case files: Knowledge management – underwriting knowledge. *CIO*. Retrieved January 25, 2004 from http://www.cio.com/archive/090102/underwriting.html

Santosus, M. (2002). Trickle up theory. *CIO*. Retrieved December 15, 2003 from http://www.cio.com/research/knowledge/edit/k041902_crm.html

Schulte, P. A. (2002). Approaches to sharing occupational safety and health information on a global scale. *American Journal of Industrial Medicine, 41*(3), 210-216.

Appendix L *(continued)*

2001

Creech, H., & Willard, T. (2001). *Strategic Intentions: Managing Knowledge Networks for Sustainable Development*. Winnipeg, Manitoba: International Institute for Sustainable Development.

Damm, D., & Schindlerb, M. (2001). Issues of a knowledge medium for distributed project work. *International Journal of Project Management*, *20*(1), 37-47.

Davenport, T. H., & Völpel, S. C. (2001). The rise of knowledge towards attention management. *Journal of Knowledge Management*, *5*(3), 212-221.

Fahey, L., Srivastava, R., Sharon, J. S., & Smith, D. E. (2001). Linking e-business and operating processes: The role of knowledge management. *IBM Systems Journal*, *40*(4), 889-907.

Gupta, A. (2001). A four-faceted knowledge-based approach to surmounting borders. *Journal of Knowledge Management*, *6*(4), 291-299.

Mitchell, M. (2001, February). Share and share alike. *Darwin*. Retrieved January 25, 2004 from http://www.darwinmag.com/read/020101/share.html?Page=1

Rubenstein-Montano, B., Buchwalter, J., & Liebowitz, J. (2001). Knowledge management: A U.S. Social Security Administration case study. *Government Information Quarterly*, *18*(3), 223-253.

Santosus, M. (2001). KM Works Magic for Ketchum. *CIO*. Retrieved January 28, 2004 from http://www.cio.com/research/knowledge/edit/ketchum.html

Santosus, M. (2001, September 1). Thanks for the memories. *CIO*. Retrieved January 25, 2004 from http://www.cio.com/archive/090101/thanks.html

Swan, J., & Scarbrough, H. (2001). Knowledge, purpose, and process: Linking knowledge management and innovation. *Proceedings presented at the 34th Hawaii International Conference on System Sciences*.

Thomas, J. C., Kellogg, W. A., & Erickson, T. (2001). The knowledge management puzzle: Human and social factors in knowledge management. *IBM Systems Journal*, *40*(4), 863-884.

Appendix L *(continued)*

von Krogh, G. (2001). The communal resource and information systems. *The Journal of Strategic Information Systems*, *11*(2), 85-107.

Wickert, A., & Herschel, R. (2001). Knowledge management issues for smaller businesses. *Journal of Knowledge Management, 5*(4), 329-337.

2000

Berkman, E. (2000, October 1). Don't lose your mind share. *CIO*. Retrieved December 15, 2003 from http://www.cio.com/

Dalrymple, P. W (2000).Knowledge management in the health sciences. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 389-402). Medford, NJ: ASIS.

Genusa, A. (2000, December 1). Chaos theory. *CIO Magazine*. Retrieved December 15, 2003 from http://www.cio.com/

Hellström, T., Kemlin, P., & Malmquist, U. (2000). Knowledge and competence management at Ericsson: Decentralization and organizational fit. *Journal of Knowledge Management, 4*(2), 99-110.

Hildreth, P., Kimble, C., & Wright, P. (2000). Communities of practice in the distributed international environment. *Journal of Knowledge Management, 4*(1), 27-38.

Levett, G. P., & Guenov, M. D. (2000). A methodology for knowledge management implementation. *Journal of Knowledge Management*, *4*(3), 258-269.

Martin, B. (2000, October). Knowledge based organizations: Emerging trends in local government in Australia. *Journal of Knowledge Management Practice*. Retrieved January 28, 2004 from http://www.tlainc.com/

Appendix L *(continued)*

Maula, M. (2000). The senses and memory of a firm – implications of autopsies theory for knowledge management. *Journal of Knowledge Management, 4*(2), 157-161.

Platt, N. (2000).Knowledge management: Can it exist in a law office? In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 405-416). Medford, NJ: ASIS.

Ryske, E. J., & Sebastian, T. B. (2000). From library to knowledge center: The evolution of a technology infocenter. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 389-402). Medford, NJ: ASIS.

Storck, J., & Hill, P. A. (2000). Knowledge diffusion through strategic communities. *Sloan Management Review, 41*(2), 63-69.

Storey, J., & Barnett, E. (2000). Knowledge management initiatives: Learning from failures. *Journal of Knowledge Management, 4*(2), 56-62.

Varon, E. (2000, August 1). The Langley Files. *CIO*. Retrieved December 15, 2003 from http://www.cio.com/archive/080100_langley.html

Wasko, M. M., & Faraj, S. (2000). "It is what one does": Why people participate and help others in electronic communities of practice. *The Journal of Strategic Information Systems*, *9*(2-3), 155-173.

Wiig, K. M. (2000). Application of knowledge management in public administration. *Knowledge Research Institute*. Retrieved January 5, 2004 from http://www.krii.com/downloads/km_in_public_admin_rev.pdf

1999

Freeman, T. (1999). Assessing innovation capacity of the consortium: An evaluation of the CAM-I cost management system program. *Journal of Knowledge Management, 3*(1), 61-65.

Appendix L *(continued)*

Galliers, B. (1999). Towards the integration of e-business, knowledge management and policy considerations within an information systems strategy framework. *The Journal of Strategic Information Systems*, *8*(3), 229-234.

Hendriks, P. H. J., & Vriens, D. J. (1999). Knowledge-based systems and knowledge management: Friends or foes? *Information & Management*, *35*(2), 113-125.

Macintosh, A., Filby, I., & Kingston, J. (1999). Knowledge management techniques: Teaching and dissemination concepts. *International Journal of Human-Computer Studies, 51*(3), 549-566.

Ramesh, B., & Tiwana, A. (1999). Supporting collaborative process knowledge management in new product Development Teams. *Decision Support Systems, 27*(1-2), 213-235.

Sieloff, C. G. (1999). “If only HP knew what HP knows”: The roots of knowledge management at Hewlett-Packard. *Journal of Knowledge Management, 3*(1), 47-53.

Simonin, B. L. (1999). Ambiguity and the process of knowledge transfer in strategic alliances. *Strategic Management Journal*, *20*(7), 595-623.

1998

Brand, A. (1998). Knowledge management and innovation at 3M. *Journal of Knowledge Management*, *2*(1), 17-22.

Buckowitz, W. (1998). At the core of a knowledge base. *Journal of Knowledge Management, 1*(3), 215-224.

Davenport, T. H. (1998). *Knowledge management case study: Knowledge management at Ernst & Young, 1997*. Retrieved October 25, 2003 from University of Texas Web site: http://www.mccombs.utexas.edu/kman/e_y.htm

Appendix L *(continued)*

Davenport, T. H. (1998). *Knowledge management case study: Knowledge management at Hewlett-Packard, early 1996*. Retrieved October 25, 2003 from University of Texas Web site: http://www.mccombs.utexas.edu/kman/hpcase.htm

Davenport, T. H. (1998). *Knowledge management case study: Knowledge management at Microsoft, 1997*. Retrieved October 25, 2003, from University of Texas Web site: http://www.mccombs.utexas.edu/kman/microsoft.htm

Davenport, T. H. (1998). *Teltech: The Business of Knowledge Management Case Study*. Retrieved October 25, 2003, from University of Texas Web site: http://www.mccombs.utexas.edu/kman/telcase.htm

Godfrey, S. (1998). Are you creative? *Journal of Knowledge Management*, *2*(1), 14-16.

Högberg, C., & Edvinsson, L. (1998). A design for futurizing knowledge networking. *Journal of Knowledge Management, 2*(2), 81-92.

Inkpen, A. C., & Dinur, A. (1998). Knowledge management processes and international joint ventures. *Journal of the Institute of Management Sciences*, *9*(4), 454-468.

Koretz, S., & Lee, G. (1998). Knowledge management and drug development. *Journal of Knowledge Management*, *2*(2), 53-58.

Pan, S. L., & Scarbrough, H. (1998). A socio-technical view of knowledge sharing at Buckman Laboratories. *Journal of Knowledge Management, 2*(1), 55-66.

Rumizen, M. C. (1998). Report on the second comparative study of knowledge creation conference. *Journal of Knowledge Management*, *2*(1), 77-81.

1997

Baker, M., & Barker, M., Thorne, J., & Dutnell, M. (1997). Leveraging human capital. *Journal of Knowledge Management, 1*(1), 63-74.

Chase, R. L. (1997a). Knowledge management benchmarks. *Journal of Knowledge Management*, *1*(1), 83-92.

Appendix L *(continued)*

Chase, R. L. (1997b). The knowledge-based organization: An international survey. *Journal of Knowledge Management, 1*(1), 38-49.

Johnson, C. (1997). Leveraging knowledge for organizational excellence. *Journal of Knowledge Management, 1*(1), 50-55.

Matthews, P. (1997). Aqua Universitas. *Journal of Knowledge Management, 1*(2), 105-112.

McConnachie, G. (1997). The management of intellectual assets: Delivering value to the business. *Journal of Knowledge Management, 1*(1), 56-62.

Rapley, K. (1997). Accounting for the value generated from innovation. *Journal of Knowledge Management*, *1*(2), 157-160.

Wiig, K. M., de Hoog, R., & van der Spek, R. (1997). Supporting knowledge management: A selection of methods and techniques. *Expert Systems with Applications*, *13*(1), 15-27.

1996

Graham, A. B., & Pizzo, V. G. (1996). A question of balance: Case studies in strategic knowledge management. *European Management Journal*, *14*(4), 338-346.

Lloyd, B. (1996). Knowledge management: The key to long-term organizational success. *Long Range Planning*, *29*(4), 576-580.

Petrash, G. (1996). Dow's journey to a knowledge value management culture. *European Management Journal*, *14*(4), 365-373.

1995

Bloom, F. E. (1995). Neuroscience-knowledge management: Slow change so far. *Trends in Neurosciences*, *18*(2), 48-49.

Appendix L *(continued)*

1995

Levinson, N. S., & Asahi, M. (1995). Cross-national alliances and interorganizational learning. *Organizational Dynamics, 24*(2), 50-63.

Appendix M

Frequency of Titles or Organizations Representing 45 Source Materials for Data Used in the First Sub-problem

Publishing title or organization	Frequency of sample documents
Journal of Knowledge Management	46
Handbook on Knowledge Management	10
CIO	7
European Management Journal	4
Journal of Knowledge Management Practice	4
Knowledge Management Case Book	4
Knowledge Management: The Catalyst for Electronic Government	4
The Journal of Strategic Information Systems	4
University of Texas	4
IBM Systems Journal	3
Information & Management	3

Appendix M *(continued)*

Publishing title or organization	Frequency of sample documents
Knowledge Management for the Information Professional	3
Decision Support Systems	2
Expert Systems with Applications	2
Futures	2
International Journal of Project Management	2
Journal of International Management	2
Technovation	2
34th Hawaii International Conference on System Sciences	1
American Journal Of Industrial Medicine	1
Association of Knowlegework	1
Business Horizons	1
Darwin	1
Government Information Quarterly	1

Appendix M *(continued)*

Publishing title or organization	Frequency of sample documents
Health	1
Industrial Marketing Management	1
International Institute for Sustainable Development	1
International Journal of Accounting Information Systems	1
International Journal of Human-Computer Studies	1
Journal of Business Research	1
Journal of Engineering and Technology Management	1
Journal of Intelligent & Fuzzy Systems	1
Journal of Knowledge Practice	1
Journal of the Institute of Management Sciences	1
Journal of World Business	1
Knowledge Research Institute	1

Appendix M *(continued)*

Publishing title or organization	Frequency of sample documents
Long Range Planning	1
Management Learning	1
Organizational Dynamics	1
Sloan Management Review	1
Strategic Management Journal	1
Swinburne University of Technology	1
The Journal of the Knowledge and Innovation Management Professional Society	1
Trends in Neurosciences	1
University of Sheffield	1

Appendix N

All Nodes and Semantic Weights (W_1) Related to Knowledge Management Using the *TextAnalyst* Default Dictionary for the 134 Data Documents

(W1)	Node
100	knowledge, management
62	Organization
52	System
47	company, business
46	Information
43	Technology
41	Strategy
39	Km
38	management system
37	knowledge management system, learning
36	Initiative
35	development
33	Activity
30	Employee
29	culture, problem
28	many, knowledge management initiative

Appendix N *(continued)*

(W1)	Node
27	two, role
26	Community
25	Area
24	manager, being, example, individual
23	performance, context, success, environment, aspect
22	three, asset, technique, concept, effort
21	management strategy, framework, perspective, product, implementation, goal
20	knowledge management strategy, creation, objective, solution, management activity
19	datum, knowledge management activity, application, human, social
18	understanding, explicit
17	et al, et, executive, idea, potential, expert, local, literature, enterprise, importance, intellectual, quality
16	working, innovation, world, relationship, making, capability, member, communication, analysis
15	several, year, information technology, industry, future, decision, knowledge asset
14	Building, common, action, internal, training, capital, specific, theory
13	Discussion, respondent, siemens, senior, method, opportunity
12	conclusion, general, current, nature, various, knowledge-based, particular, database, four, intellectual capital

Appendix N *(continued)*

(W1)	Node
11	competency, awareness, practitioner, skill, possible, others, finding, ability, doe, operation, infrastructure, intranet, might, source, significant
10	necessary, means, vision, business strategy, professional, way, introduction, fact, user, crisplant, government, improvement, mechanism, external, explicit knowledge, main, worker, tacit knowledge
9	personal, management , effort, knowledge management effort, management of knowledge, department, meeting, customer, basis, principle, knowledge creation, hp, generation
8	cent, insight, responsibility, collective, growth, person, unit, health, policy, leading, attention, personnel, definition, implication, integration, participant, davenport, office, software, interaction, active
7	thing, organizational , knowledge, corporation, boundary, epistemology, requirement, academic, variety, primary, investment, authority, basic, central, director, few, steps, aspect of knowledge, national, infineon, domain, relation, journal, managing knowledge, emphasis, leader, outcome, american, category, characteristic, public, global knowledge, client, computer
6	researcher, collaboration, swiss, commitment, foundation, intelligence, management and learning, setting, valuable, five, management framework, organizational culture, apqc, dissemination, cannot, marketing, essential, growing, topic, links, contribution, international, great, kecnetworking, kind, day, beginning, similar, leadership, response, effectiveness, direction, whole

Appendix N *(continued)*

(W1)	Node
5	infineon technology ag, recognition, language, learning and knowledge, taking, local government, material, third, behavior, journal of knowledge management, nonaka, knowledge management problem, keyword, doing, generation knowledge management, repository, benchmarking, engineering, small, knowledge worker, kecnetworking - knowledge management at infineon technology ag, knowledge management framework, knowledge management technology, productivity, science, management technique, codification, loss, component, private, information system, thinking, country, standard, organizational learning, architecture, hr, knowledge management and learning, knowledge strategy, thought, becoming, ssa, internet, dynamic, situation, customers, management literature, procedure, buckman, aspect of knowledge management, platform, paradigm, laboratory, six, overview, alliance, sale
4	motivation, conference, dealing, information management, strategic business, extent, economy, icn, consultant, driver, australia, business objective, librarian, intangible, ict, assumption, virtual enterprise, knowledge manager, successful knowledge management, importance of knowledge, etc, corporate knowledge, difficulty, identification, workshop, existence, production, knowledge management action, entire, intervention, costs, perception, distribution, learning organization, transformation, [nature of knowledge, methodology, management action, facilitator, positive], efficient, knowledge-intensive, implementation of knowledge management, movement, epistemological, connection, knowledge management capability, knowledge management technique, utilization, meaning, complex, story, knowledge management literature

Appendix N *(continued)*

(W1)	Node
3	global knowledge management, life, modeling, deployment, internal and external, based organization, privacy, certain, participation, chief, agendum, acquisition, notion, product development, knowledge and knowledge, soleunet, rjvs, possibility, adopter, fundamental, knowledge management principle, gabbay et al, teaching, autopoietic, local authority, ten, dr, political, based knowledge, senior manager, many knowledge, analyzing, buckman laboratory, decision making, epistemologies, competence, terminology, summary, series, rjv, volume, presentation, telecommunication, percent, strategic business objective, business unit, measurement, bases, area of knowledge, definition of knowledge management, significance, capacity, commercial, personalization, sustainable, knowledge-based organization, knowledge area, knowledge-based system, pdp, based system, society, complexity, location, forum, corporate knowledge management, criterion, hypothesis, region, concept of knowledge, knowledge and performance, medium, education, knowledge management solution, belief, young, library, simple, scenario, definition of knowledge, actual, com, competitiveness, division, management business, european, module, cooperation, knowledge management and knowledge, responsible for knowledge management, expectation, assessment, addition, period, senior management, role of knowledge, variable, feedback, marketplace, specific knowledge, competitor, prusak, description, information and knowledge

Appendix N *(continued)*

(W1)	Node
2	excellence, importance of knowledge management, autopoietic epistemology, lotus, dow, consultancy, creation of knowledge, business environment, swan, usa, words, knowledge management product, hedlund, knowledge management theory, attitude, going, uk, groupware, colleague, der spek, strategy for knowledge management, associated with knowledge, old, business intelligence, critical success, organizational context, flexibility, involvement, agency, networking, collective knowledge, pharmaceuticals, loss of knowledge, behavior, presence, different knowledge, evolution, conversation, factory, method and technique, executive management, proficiency, intellectual property, priority, bri, observation, kind of knowledge, km initiative, phenomenon, knowledge development, knowledge and knowledge management, metrics, social knowledge management, structuring, crisplant's knowledge management, multiple, works, federal, motorola, theme, ii, partnership, workforce, error, formative knowledge, living, enabler, hp consulting, pursuit, guidance, knowledge management goal, energy, output, entity, knowledge-hoarding, communication technology, preliminary, pac, pressure, special, pp, road, knowledge management business strategy, shareholder, usage, adoption, collection, agent, awareness of knowledge management, ambition, depth, knowledge community, ernst, personalization strategy, schneider, tangible, alternative, small company, conversion, obstacle, designing, drawing, nonaka and takeuchi, internal knowledge, skandia, problem of knowledge, sustained strategic commitment, artifact, ibm, comparison, formal knowledge, news, many knowledge management, mentoring, europe, choice, selection, implicit knowledge, manufacturing, construction, consideration, kbs, mapping, linkage, reality, failure, familiar, diffusion, davenport and prusak, iii, knowledge management intervention, different epistemologies, maintenance, remains, actor, formation, one, mechanism for knowledge, thomas, responsibility for knowledge, integral, scarbrough, norm, socio-technical, corporate culture, stakeholder, questionnaire

Appendix N *(continued)*

(W1)	Node
2	parent, ideal, mode, relevance, creative working, www, rm consulting, university, knowledge loss, incentive, formal knowledge management, storing, president, orientation, japanese, realization, unique, philosophy, addressing, imperative, missing, industrial, driving, suggestion, wiig, achievement, important role, asia, carrying, rainbow, teamwork, http, decade, creativity, combination, hewlett-packard, quality management, mid, digital, ve, astrazeneca, important knowledge, lds, strengthening, knownet, impossible, million, australian, physical, century, writing, specialist, recent year, facing, memory, property, company knowledge, role of knowledge management, reader, cisco, retrieval, benchmark, exploration, kms, important aspect, investigation, council, establishment, considerable, intellectual asset, consortium, goal of knowledge management, poor, success of knowledge management, hoarding, takeuchi, evaluation, knowledge bases, taxonomy, reinsurance, representative, teaching and dissemination, knowledge economy, committee, socialization, lawyer, gsa, specific knowledge management, intention, determinant, helping, responsibility for knowledge management, information and communication

Appendix O

Themes and Dependent Words Used in *TextAnalyst's* Custom Dictionary

Theme	Dependent words
knowledge management	governance, km, kms, leadership, management, managing, vision
Knowledge	advice, data, datum, expertise, idea, ideas, information, insight, insights, intellect, intellectual, intelligence, intuition, judgment, know-how, wisdom
Organization	business, businesses, companies, company, corporation, corporations, department, departmental, departments, enterprise, enterprises, entities, entity, industries, industry, office, offices, operation, organizational. organizations, social, societal, society
System	architecture, architectures, framework, frameworks, infrastructure, infrastructures, kbs, knowledge-based system, mechanisms, method, methodologies, methodology, methods, procedure, procedures, process, processes, strategic, strategies, strategy, structure, structures, systems
Technology	artificial intelligence, computer, computer technology, computers, computing, data processing, information retrieval, information technology, mainframe, mainframes, neural net, neural network, neural networks, operating systems, pc, pcs, technologic, technologies, telecommunication, telecommunications, tools, tool, workstation, workstations

Appendix O *(continued)*

Theme	Dependent words
Learning	assimilate, awareness, competence, competency, comprehend, comprehension, discover, discoveries, discovery, educate, educates, education, instruct, instructing, instruction, instructs, learn, learner, novice, skill, skills, teach, teaching, train, training, understand, understanding
Culture	attitude, attitudes, behavior, behaviors, belief, beliefs, commitment, commitments, countries, country, cultural, cultures, customs, ethic, ethics, norm, norms, political, social, societal, societies, society, socio-cultural, tradition, traditions, values, trust
Individual	actor, actors, agent, agents, apprentice, ceo, chief executive officer, chief information officer, chief knowledge officer, cio, cko, colleague, colleagues, consultant, consultants, director, directors, employee , employees, end-user, end-users, executive, executives, expert, experts, facilitator, facilitators, friends, human, individuals, leader, learner, leaders, librarian, librarians, manager, managers, member, members, novice, participant, participants, people, person, personal, personnel, practitioner, practitioners, specialist, specialists, stakeholder, stakeholders, student, students, teacher, teachers, user, users, worker, workers
Performance	abilities, ability, achievement, capabilities, capability, creation, creations, development, developments, effective, effectiveness, improvement, improvements, improving, innovate, innovates, innovation, problem, problems, productivity, qualities, quality, solution, solutions, value

Appendix O *(continued)*

Theme	Dependent words
Policy	directive, directives, doctrine, guideline, guidelines, ideologies, ideology, philosophies, philosophy, policies, standards, tenet, tenets
Diffusion	circulate, circulates, circulating, collaborate, collaborates, collaboration, communicate, communicates, communication, conference, conferences, conversation, conversations, cooperation, diffuse, diffusing, discussion, discussions, disperse, disseminate, dissemination, distribution, flow, flows, forum, forums, inform, interaction, interactions, link, linkage, linkages, links, meeting, meetings, participate, participates, participation, partnership, partnerships, share, shared, shares, sharing, socialization, socialize, spread, spreading, spreads, transfer, transference, transferred, transferring, transfers, transmission, transmissions, workshop
Disclosure	access, accessed, accessing, anonymous, concealed, confidential, confidentiality, disclose, disclosed, disclosing, divulging, expose, identification, identifying, identity, leak, leakage, privacy, private, proprietary, protect, protects, reveal, reveals, secrecy, secret, secrets, security, unauthorized
community of practice	alliance, alliances, association, associations, coi, communities, community, cop, kc, peer groups, pools
network of practice	community of interest, net, network, networked, networking, networks

Appendix P

Common and Deleted Words Used in *TextAnalyst's* Custom Dictionary

Type	Words
Common	academic, acquisition, action, agency, agreement, ambiguity, analysis, analyst, analyzing, application, assessment, asset, attention, audience, authority, benchmarking, building, capacity, capital, catalyst, category, characteristic, client, codification, collection, collective, committee, competition, competitiveness, competitor, complex, complexity, component, concept, conclusion, connection, consumer, context, costs, customer, database, decision, definition, delivery, digital, direction, division, domain, dynamic, economy, efficiency, efficient, effort, embeddedness, engineering, environment, evaluation, example, explicit, external, fact, failure, feedback, future, generation, goal, government, hr, hrm, implementation, indicator, infocenter, initiative, integration, internal, international, Internet, Intranet, investment, language, library, local, location, material, meaning, means, measurement, national, nature, objective, opportunity, orientation, outcome, party, platform, portal, possible, potential, presentation, processing, production, professional, property, public, recognition, region, relation, relationship, repository, requirement, researcher, respondent, response, responsibility, senior, situation, software, source, standard, story, supplier, sustainable, synergy, technique, theory, thinking, thought, topic, transformation, university, utilization, valuable, video, words, world

Appendix P *(continued)*

Type	Words
Deleted	active, activity, actual, addition, ag, agendum, al, alternative, American, area, Arthur, aspect, assumption, availability, balanced, based, bases, basis, basic, becoming, beginning, being, bri, Buckman, cannot, cent, central, certain, certification, chemical, choice, Cisco, combination, commercial, common, considerable, consideration, construction, contribution, conversion, Crisplant, criterion, current, Davenport, day, dealing, dependent, deployment, depth, description, designing, distinction, DOE, doing, driver, emphasis, entire, episode, Ericsson, essential, et, et al, etc, existence, expectation, extent, few, finding, five, foundation, four, fundamental, general, great, growing, growth, GSA, health, helping, history, HP, ICT, implication, importance, intangible, intention, introduction, involving, Japanese, journal, JV, keeping, kind, KMM, laboratory, lds, leading, life, literature, loss, lotus, main, majority, maker, making, manner, manual, manufacturing, many, marketing, Microsoft, might, military, mode, month, multiple, necessary, Nonaka, notion, observed, old, one, original, others, output, overview, PAC, para, paradigm, parent, particular, path, percent, period, perspective, physical, portfolio, positive, primary, principle, prior, priority, private sector, product, proposal, Prusak, putting, rapid, regression, relevance, revenue, role, sale, scoreboard, sector, selection, setting, several, Siemens, significant, similar, simple, six, small, special, specific, SSA, steps, strength, success, summary, Swiss, Takeuchi, taking, Teltech, ten, thing, third, three, Tom, two, unique, unit, variable, variety, various, volume, von, von Krogh, way, whole, working, year, young, Zopps

Appendix Q

Semantic Weight (W) and Sentence Frequency (S_f) for Thematic Pairs Used in the Taxonomy of KM

	KM		Diffusion		Disclosure		Policy	
Taxonomy	W	S_f	W	S_f	W	S_f	W	S_f
Knowledge	89	3,770	71	4,160	33	737	13	207
Organization	79	2,418	69	2,333	32	425	17	170
System	77	2,195	70	1,961	34	399	21	190
Performance	72	1,807	71	1,901	32	332	20	168
Individual	71	1,777	74	2,695	35	489	17	168
Learning	56	922	70	1,132	30	186	14	67
Technology	51	726	72	722	37	160	14	40
Culture	49	693	75	999	33	155	17	66
Network of practice	12	428	73	761	31	118	24	84
Community of practice	36	381	75	860	32	129	14	43

Appendix U

Standardized Open-ended Interview Questions

used in the Second Sub-problem

Introduction

a. *Please describe your background, experiences, or knowledge as related to any aspect of collecting and sharing airline safety data or information.*

Knowledge Management

a. *Do you or affiliate organization(s) have structures or processes for sharing aviation safety information? If so, could you provide an overview of those structures or processes?*
b. *How do you or your affiliates identify needed information or select sources of information?*
c. *Do you align and evaluate information with the needs of your mission or organizational function?*
d. *How do you identify individuals or entities that are willing to support or help manage your aviation safety information sharing efforts?*
e. *What management processes or strategies might you use to create a culture that supports sharing aviation safety information?*
f. *What strategies or processes might you recommend for collecting, storing, and disseminating aviation safety information?*
g. *What kinds of systems or technologies are used by you or your affiliates or might you recommend to facilitate collecting, storing, and disseminating airline safety information?*
h. *How should collected and stored aviation safety information be made visible in relation to awareness and access by potential users?*
i. *How might incentives or motivations be used to encourage individuals or entities to share aviation safety information?*

Appendix U *(continued)*

j. *Can you describe any efforts or systems enabling stakeholders to analyze or learn from shared aviation safety information?*

k. *If applicable, please describe your or your organization's involvement in communities or networks of practice.*

l. *What do you believe are the major challenges for implementing or managing the sharing of aviation safety information? What solutions have you considered or implemented for those problems or challenges? For those solutions implemented, how effective have they been?*

Diffusion

a. *Can you recommend or describe strategies or processes for enhancing the diffusion of aviation safety information?*

b. *What methods, processes, or systems are successful for diffusing aviation safety information among organizations or different cultures?*

c. *How important is socialization or face-to-face interaction to the sharing of aviation safety information?*

d. *Can you describe known or potential barriers to the diffusion of aviation sharing information? Do you know of existing solutions or can you recommend potential solutions to these barriers?*

e. *Can you describe observations or experiences related to selecting, integrating, or using systems designed for diffusing aviation safety information?*

f. *Can you describe ways to measure or demonstrate the impact of diffusing aviation safety information on issues related to individual or organizational performance?*

g. *Can you describe ways to determine the viability of cultures or organizations to be receptive to, or sustain knowledge diffusion?*

h. *Can you describe ways to evaluate the effectiveness of diffusing aviation safety information through networks or communities of practice?*

i. *What challenges have you experienced or observed in sharing aviation safety information within or among communities or networks of practice?*

Appendix U *(continued)*

Disclosure

a. *Can you describe strategies or processes enhancing access to existing or potential sources of aviation safety information or knowledge?*
b. *Can you describe strategies or processes that secure or prevent access to the identity of individuals or organizations contributing or sharing aviation safety information or knowledge?*
c. *Can you describe laws, regulations, cases, policies, or processes that serve to protect the identity of individuals or organizations providing aviation safety information? Can you describe known or potential risks of disclosure as related to these examples?*
d. *Can you describe systems, processes, or technologies that intentionally or unintentionally enable the identification of sources to aviation safety information?*
e. *Can you describe systems, processes, or technologies that serve to protect the identification of individuals or organizations that provide aviation safety information?*
f. *Are there known or potential risks of disclosure related to technologies used in aviation safety information sharing systems or processes?*
g. *How can aviation safety information sharing programs manage risks inherent to personal interaction (e.g. face-to-face meetings) with the need for anonymity or confidentiality?*

Policy

a. *Can you describe policies or philosophies related to the diffusion of aviation safety information and protecting the identification of sources of that information? Are there recommendations you can make regarding policies that should be developed for disseminating aviation safety information?*
b. *To your knowledge, are policies or philosophies made clear to all stakeholders participating in aviation safety information sharing programs or processes?*
c. *What are the best ways to disseminate policies or philosophies related to aviation sharing information programs to participants?*

Appendix U *(continued)*

d. *Are you involved in the development of policies related to aviation safety information sharing programs you or your affiliates participate in?*

e. *Are there policies that govern the standards or usability of technologies used in the aviation sharing programs or systems you or your affiliates participate in?*

f. *Have you observed or experienced strategies for sharing policies across various cultures participating in aviation safety information sharing programs? How successful have those processes been?*

g. *Can you describe policies specific to participating in and sharing information within networks or communities of practice? Do you have any examples of how different communities or networks have reconciled varying policies in order to share information or knowledge?*

Conclusion

a. *What specific recommendations can you suggest for managing the impact of disclosure on the diffusion of airline safety information?*

Reference List

Abou-Zeid, E.-S. (2002). A knowledge management reference model. *Journal of Knowledge Management, 6*(5), 486-499.

Addleson, M. (2000). Organizing to know and to learn: Reflections on organization and knowledge management. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 137-160). Medford, NJ: ASIS.

Alvarez, J. L. (Ed.). (1998). *The Diffusion and Consumption of Business Knowledge*. New York: St. Martin's Press.

Ambrose, S. E. (2000). *Nothing Like It in the World*. New York: Simon & Schuster.

American Medical Association. (2003). *Peer Review*. Retrieved June 21, 2003 from http://www.ama-assn.org/ama/pub/printcat/8114.html

Anderson, C. J., Glassman, M., & Pinelli, T. E. (1997). The relationship between technical uncertainty and information use by industry-affiliated U.S. aerospace engineers and scientist. In T. E. Pinelli, R. O. Barclay, J. M. Kennedy, & A. P. Bishop, (Eds.), *Knowledge Diffusion in the U.S. Aerospace Industry: Managing Knowledge for a Competitive Advantage* (Parts A-B) (pp. 325-378). Greenwich, CT: Ablex Publishing.

Anderson, D. J., & Webster, C. S. (2001). A systems approach to the reduction of medication error on the hospital ward. *Journal of Advanced Nursing*, *35*(1), 34-41.

Andrén, G. (1981). Reliability and content analysis. In K. E. Rosengren, (Ed.), *Advances in Content Analysis* (pp. 43-67). Beverly Hills, CA: Sage.

Andrus, C. H., Villasenor, E. G., Kettelle, Roth, R., Sweeney, A. M., & Matolo, N. M. (2003). "To err is human": Uniformly reporting medical errors and near misses, a naïve, costly, and misdirected goal. *American College of Surgeons, 196*(6), 911-918.

Angerand, L. (2000, June). What can governments do to help GAIN? A paper presented at the meeting of the Fourth GAIN World Conference, Paris, France.

Ardichvili, A., Page, V., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management*, *7*(1), 64-77.

Auditore, P. J. (2002, January). Enabling knowledge management in today's knowledge economy. *KMWorld*, S8.

Auditore, P. J. (2003, June). Governments worldwide poised to exploit knowledge management. *KMWorld* [Special Supplement], S4-S5.

Australia. Attorney-General's Department. (2003). *Australian Freedom of Information Act 1982*. Retrieved July 14, 2003 from http://scaleplus.law.gov.au/html/pasteact/0/58/top.htm

Australia. Transport Safety Bureau. (2002, September 16). Confidential Aviation Incident Reporting (CAIR). Retrieved September 28, 2002 from http://www.atsb.gov.au/aviation/index.cfm#

Aviation Safety Institute. (2002). *Our History*. Retrieved October 3, 2002 from http://www.aero-farm.com/asi/history.htm

AvSoft. (2003). *What is AvShare?* Retrieved August 16, 2003 from http://www.avsoft.co.uk/index.html

Baker, M., Barker, M., Thorne, J., & Dutnell, M. (1997). Leveraging human capital. *Journal of Knowledge Management, 1*(1), 63-74.

Barach, P., & Small, S. D. (2000). Reporting and preventing medical mishaps: Lessons from non-medical near miss reporting systems. *BMJ, 320,* 759-763.

Barclay, R. O., & Murray, P. C. (1997). What is knowledge management? *Knowledge Praxis*. Retrieved January 13, 2002 from http://www.media-access.com/whatis.html

Barclay, R. O., & Pinelli T. E. (1997). Diffusing federally funded aeronautical research and technology – Toward a knowledge management structure. In T. E. Pinelli, R. O. Barclay, J. M. Kennedy, & A. P. Bishop, (Eds.), *Knowledge Diffusion in the U.S. Aerospace Industry: Managing Knowledge for a Competitive Advantage* (Parts A-B) (pp. 891-948). Greenwich, CT: Ablex Publishing.

Barquin, R. C. (2003). What is knowledge management? In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 285-300). Vienna, VA: Management Concepts.

Barquin, R. C., Bennet, A., & Remez, S. G. (2003).The GSA story: Swimming with the dolphins. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 453-468). Vienna, VA: Management Concepts.

Barth, S. (2004). Integrating knowledge management and competitive intelligence; integrating offense and defense. In M. E. D. Koenig & T. K. Srikantaiah (Eds.), *Knowledge Management Lessons Learned* (pp. 461-481). Medford, NJ: ASIS.

Basler, R. B. (Ed.). (1953-1955). *The Collected Works of Abraham Lincoln (Vols. 1-9)*. New Brunswick, NJ: Rutgers University Press.

Baumgarner, J. (2002). Sharing of safety information gains momentum. *Aviation Daily, 347*(4), 5.

Beckman, T. (2003). Creating business value from knowledge management. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 49-96). Vienna, VA: Management Concepts.

Bell, M. (2000). Rethinking ‘useful’ knowledge. In J. R. Bryson, P. W. Daniels, N. Henry, & J. Pollard (Eds.), *Knowledge, Space, Economy* (pp. 191-205). New York: Rutledge.

Bennet, D., & Bennet, A. (2003). The rise of the knowledge organization. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 25-48). Vienna, VA: Management Concepts.

Bennet, A., & Neilson, R. (2003). The leaders of knowledge initiatives: Qualifications, roles, and responsibilities. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 523-538). New York: Springer.

Bennet, A., & Porter, D. (2003). The force of knowledge, a case study of KM implementation in the Department of the Navy. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 467-487). New York: Springer.

Benoist, Y. (1998, November). *Airbus Views and Current Activities on Data Sharing*. Paper presented at the meeting of the Third GAIN World Conference, Long Beach, California.

Berdrow, I., & Lane, H. W. (in press). International joint ventures: Creating value through successful knowledge management. *Journal of World Business*.

Beveren, J. V. (2003). Does health care for knowledge management. *Journal of Knowledge Management, 7*(1), 90-95.

Billings, C. (1998). *Incident Reporting Systems in Medicine and Experience with the Aviation Safety Reporting System.* Report from a Workshop on Assembling the Scientific Basis for Progress on Patient Safety, National Patient Safety Foundation at the AMA. Retrieved May 4, 2003 from http://www.npsf.org/exec/billings.html

Blakey, M. C. (2003). FAA Speeches by Marion C. Blakey, Federal Aviation Administer. *U.S. Federal Aviation Administration.* Speech presented at the European Aviation Club, Brussels, Belgium, June 18, 2003. Retrieved August 29, 2003 from http://www1.faa.gov/index.cfm/apa/1223/

Boland, R. J., & Yoo, Y. (2003). Sensemaking and knowledge management. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 381-392). New York: Springer.

Booker, G. (1997, May). *Minutes of the Second Global Analysis and Information Network (GAIN) Conference*. Symposium conducted at the meeting of the Second GAIN World Conference, London, England.

Borko, H. (1968). Information science: What is it? *American Documentation*, *19*(1), 3-5.

Bozin, B. (1998, November). *Steering Committee Strawman: The Way Ahead for GAIN*. Paper presented at the meeting of the Third GAIN World Conference, Long Beach, California.

Brand, A. (1998). Knowledge management and innovation at 3M. *Journal of Knowledge Management*, *2*(1), 17-22.

Brauner, E., & Becker, A. (2006). Knowledge management in interaction: Transactive knowledge systems and the management of knowledge. In B. Renzl, K. Matzler, & H. Hinterhuber, (Eds.), *The Future of Knowledge Management* (pp. 62-81). New York: Palgrave Macmillan.

Bresnen, M., Edelman, L., Newell, S., Scarbrough, H., & Swan, J. (2003). Social practices and the management of knowledge in project environments. *International Journal of Project Management*, *21*(3), 157-166.

Brown, D. B., Parrish, A., Vrbsky, S., Dixon, B., & Gainer, C. (1999). *An Information Mining Approach Toward Improving Aviation Safety*. Proceedings presented at the 1999 Fifth ISSAT International Conference on Reliability and Quality in Design. Retrieved September 15, 2002 from http://care.cs.ua.edu/docs/issat.pdf

Brown, J. S., & Duguid, P. (2000). *The Social Life of Information*. Boston: Harvard Business School Press.

Brown, R. D. (1989). *Knowledge is Power*. New York: Oxford University Press.

Brown, R. D. (2000). Early American Origins of the Information Age. In A. D. Chandler, & J. W. Cortada, (Eds.), *A Nation Transformed by Information* (pp. 39-54). New York: Oxford University Press.

Buckholtz, T. J. (1995). *Information Proficiency*. New York: VNR.

Buckowitz, W. R., & Williams, R. L. (2000). *The Knowledge Management Fieldbook*. London: Prentice Hall.

Bureau d'Enquêtes et d'Analyses. [2002]. *Presentation of the REC*. Retrieved on August 31, 2002 from http://www.bea-fr.org/anglaise/rec_cers.htm

Burger, R. H. (1993). *Information Policy: A Framework for Evaluation and Policy Research*. Norwood, NJ: Ablex.

Burin, J. (2003, June). *Protection of the Sources of Safety Information*. Paper presented at the meeting of the Sixth GAIN World Conference, Rome, Italy.

Burk, M. (2002). Federal Highway Administration knowledge sharing success story: Rumble strips government-to-government community of practice. *The Journal of the Knowledge and Innovation Management Professional Society, 1*(1). Retrieved January 4, 2004 from http://www.kmpro.org/journal/Vol1_No1_Dec02/industry_focus.cfm

Burke, P. (2000). *A Social History of Knowledge*. Cambridge, UK: Polity.

Campaign for Freedom of Information. [2001]. *Welcome to the Campaign for Freedom of Information*. Retrieved September 28, 2002 from http://www.cfoi.org.uk/

Canada. (1998). *Access to Information Act*. Retrieved September 26, 2002 from http://infosource.gc.ca/Info_4/atip/Access-Brochr_e.html

Canada. British Columbia Office of the Information and Privacy Commissioner. (2003). *Your Information and Privacy Rights*. Retrieved July 16, 2003 from http://www.oipcbc.org/citizens/info_privacy_guide.php

Canada. Department of Justice. (2003). *Access and Privacy Laws and Commissions*. Retrieved July 16, 2003 from http://canada.justice.gc.ca/en/ps/atip/provte.html

Canada. Ontario Information and Privacy Commissioner. (2003). *A Mini Guide to Ontario's Freedom of Information and Protection of Privacy Act*. Retrieved July 16, 2003 from http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11601&N_ID=1&PT_ID=23&U_ID=0

Canada. Transport Canada. (2002). *System Safety Evaluation*. Retrieved September 27, 2002 from http://www.tc.gc.ca/Quebec/en/aviationSafety/evaluation.htm#CADORS

Canada. Transport Canada. (2003d). *Welcome to the Transport Canada Web Service Difficulty Reporting System (WSDRS)*. Retrieved July 26, 2003 from http://www.tc.gc.ca/wsdrs/

Canada. Transportation Safety Board of Canada. (2001). *SECURITAS*. Retrieved September 27, 2002 from http://www.tsb.gc.ca/ENG/

Caterinicchia, D. (2001). High tech to the forefront. *Federal Computer Week*. Retrieved December 8, 2002 from http://www.fcw.com/fcw/articles/2001/1015/cov-econbar2-10-15-01.asp

Chabrow, E. (1999). Editor's note: Transferring knowledge. *Informationweek Online*. Retrieved January 13, 2002 from http://www.informationweek.com/731/31eredn.htm

Chandler, A. D., & Cortada, J. W. (Eds.). (2000). *A Nation Transformed by Information*. New York: Oxford University Press.

Chase, R. L. (1997). Knowledge management benchmarks. *Journal of Knowledge Management, 1*(1), 83-92.

Christensen, C. H., & Bang, H. K. (2003). Knowledge management in a project oriented organization: Three perspectives. *Journal of Knowledge Management, 7*(3), 116-128.

Chuang, S.-H. (2004). A resource-based perspective on knowledge management capability and competitive advantage: An empirical investigation. *Expert Systems with Applications*, *27*(3), 459-465.

CiteSteer. (2002). *Citations: Knowledge Management*. Retrieved on November 26, 2002 from http://citeseer.nj.nec.com/context/1205523/0

Clark, T. (1998). *Just a few anticipated cost benefits of FOQA*. Retrieved July 14, 2002 from http://www.gainweb.org/

Clarke, D. B. (2000). Space, knowledge, and consumption. In J. R. Bryson, P. W. Daniels, N. Henry, & J. Pollard (Eds.), *Knowledge, Space, Economy* (pp. 209-225). New York: Rutledge.

Cleveland, H. (1985). *The Knowledge Executive*. New York: Dutton.

Cohen, M. R. (2000). Why error reporting systems should be voluntary. *BMJ, 320*, 728-729.

Communications Law Centre. (2000). *Information Equity*. Retrieved September 28, 2002 from http://www.comslaw.org.au/research/Equity/19990924_elwoodfoi.html

CompuServe. (2002). *AVSIG*. Retrieved October 3, 2002 from http://forums.compuserve.com/gvforums/default.asp?SRV=Avsig

Confidential Human Factors Reporting Program. [2001]. *What is CHIRP?* Retrieved September 29, 2002 from http://www.chirp.co.uk

Contractor, F. J., & Ra, W. (2002). How knowledge attributes influence alliance governance choices. *Journal of International Management*, *8*(1), 11-27.

Conway, S. (2003). Building a KM foundation at Microsoft Consulting Services. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 565-576). New York: Springer.

Cornelius, I. (1996). *Meaning and Method in Information Studies*. Norwood, NJ: Ablex.

Cortada, J. W. (2000). Progenitors of the Information Age. In A. D. Chandler, & J. W. Cortada, (Eds.). *A Nation Transformed by Information* (pp. 177-216). New York: Oxford University Press.

Creech, H., & Willard, T. (2001). *Strategic Intentions: Managing Knowledge Networks for Sustainable Development*. Winnipeg, Manitoba: International Institute for Sustainable Development.

Critical Infrastructure Information Act or 2002, H.R. 5005, 107th Cong, § 211 (2002).

Crowley, B. (2000). Tacit knowledge and quality assurance: Bridging the theory-practice divide. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 205-220). Medford, NJ: ASIS.

Currie, G., & Kerrin, M. (2004). The limits of a technological fix to knowledge management. *Management Learning, 35*(1), 9-29.

Dalrymple, P. W. (2000). Knowledge management in the health sciences. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 389-402). Medford, NJ: ASIS.

Dalton, J., Glenn, M., Wojciech, J., Parker, R., Romanowski, M., & Chang, G. (1997). GAIN Working Group I Committee report information sharing proof of concept. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 8.1-8.21). London: Royal Aeronautical Society.

Damm, D., & Schindlerb, M. (2001). Issues of a knowledge medium for distributed project work. *International Journal of Project Management*, *20*(1), 37-47.

Davenport, E., & Cronin, B. (2000). Knowledge management: Semantic drift or conceptual shift? *ALISE*. Retrieved April 16, 2001 from http://www.alise.org/conferences/conf00_Davenport-Cronin_paper.htm

Davenport, T. (1997). *Information Ecology*. New York: Oxford University Press.

Davenport, T., & Prusak, L. (2000). *Working Knowledge* (Rev. ed.). Boston: Harvard Business School Press.

Davenport, T. H., & Völpel, S. C. (2001). The rise of knowledge towards attention management. *Journal of Knowledge Management*, *5*(3), 212-221.

de Courville, B. (2001). *How governments can support the airlines*. Retrieved August 17, 2002 from http://www.gainweb.org/

Debons, A., & Horne, E. E. (1998). NATO Advanced Study Institutes of Information Science and foundations of information science. In T. B. Hahn & M. Buckland, (Eds.). *Historical Studies in Information Science* (pp. 205-214).Medford, NJ: ASIS.

Delmater, R., & Hancock, M. (2001). *Data Mining Explained*. Boston: Digital Press.

Denning, S. (2000). History of knowledge management. *Stephen Denning*. Retrieved January 21, 2002 from http://www.stevedenning.com/history_knowledge_management.html

Denning, S. (2003). Knowledge sharing at the World Bank. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 469-484). Vienna, VA: Management Concepts.

Desouza, K. C. (2003). Knowledge management barriers: Why the technology imperative seldom works. *Business Horizons*, *46*(1), 25-29.

Despres, C., & Chauvel, D. (Eds.). (2000a). *Knowledge Horizons*. Boston: Butterworth Heinemann.

Despres, C., & Chauvel, D. (2000b). A thematic analysis of the thinking in knowledge management. In C. Despres & D. Chauvel (Eds.). *Knowledge Horizons* (pp. 55-86). Boston: Butterworth Heinemann.

DeTore, A. W., & Balliet-Milholland, J. M. (2003). Transforming theory into fact: Hands-on knowledge management initiatives built on a Reinsurer's pile of junk. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 533-547). New York: Springer.

Doguet, R. (1998). *Implementing a multi-channel feedback system*. Retrieved July 14, 2002 from http://www.gainweb.org/

Doherty, M., Lau, M. S., Kaur, S., & Jain, R. (2005). Using ontologies to improve knowledge management in technology transfer. *International Journal of Technology Transfer and Commercialization*, *4*(1), 105-125.

Douglass, M., Clifford, G. D., Reisner, A., Moody, G. B., & Mark, R. G. (n.d.). Computer-assisted de-identification of free text in the MIMIC II Database. Retrieved on January 8, 2006 from Harvard-MIT Division of Health Sciences & Technology, MIMIC-MIT Web site: http://mimic.mit.edu/Archive/Papers/MDouglass.pdf

Dueck, G. (2001). Views of knowledge are human views. *IBM Systems Journal, 40*(4), 885-888.

Duquette, A. (2002). Fact sheet: Air transportation oversight system (ATOS) evaluation. *FAA News*. Retrieved September 1, 2002 from http://www.faa.gov/apa/FACTSHEET/2002/fact1Jan.htm

EUCARE. (1995). *EUCAREVIEW 6*. Retrieved October 4, 2002 from http://aviation-safety.net/pubs/eucare/ecview6.htm

EUCARE. [2000]. *What is EUCARE?* Retrieved August 26, 2002 from http://www.eucare.de/whatis.htm

European Commission. (2002). European Parliament and Council Directive 2002/…/EC on occurrence reporting in civil aviation. *IFATSEA*. Retrieved August 6, 2003 from http://www.mooney.demon.co.uk/eurogroup/Safety_Day/01%20-%20IFATSEA%20Safety%20Awareness%20day%2026%20Nov%202002%20Report.pdf

Fahey, L., Srivastava, R., Sharon, J. S., & Smith, D. E. (2001). Linking e-business and operating processes: The role of knowledge management. *IBM Systems Journal, 40*(4), 889-907.

Fang, S., Hong, K., Bock, G. W., & Kim, I. (2002). Knowledge management and process innovation: The knowledge transformation path in Samsung SDI. *Journal of Knowledge Management, 6*(5), 479-485.

Fattori, M., Pedrazzi, G., & Turra, R. (2003). Text mining applied to patent mapping: A practical business case. *World Patent information*, *25*, 335-342.

Federal Aviation Administration Reauthorization Act of 1996, 104 U.S.C. § 402 (1996).

Federal Republic of Germany. (2003). *Informationsfreiheit in Deutschland*. Retrieved August 23, 2003 from http://www.informationsfreiheit.de/info_deutschland/index.htm

Ferrari, F. M., & Carlos de Toledo, J. (2004). Analyzing the knowledge management through the product development process. *Journal of Knowledge Management, 8*(1), 117-129.

Firestone, J. M., & McElroy, M. W. (2003). *Key Issues in the New Knowledge Management*. New York: Butterworth Heinemann.

Flash, C. (2000). Knowledge management meets the portal. Interview with J. Jacobs. *Datamation*. Retrieved January 12, 2002 from http://216.239.37.100/search?q=cache:DGyzbaGbPsEC:softwaredev.earthweb.com/article/0,,10454_622751,00.html+Knowledge+Management+Meets+the+Portal&hl=en&ie=UTF-8

Flight Operational Quality Assurance Program (FOQA), 14 C.F.R. § 193 (2003).

Foley, K. (2001). Knowledge management key to collaboration. *Informationweek.com*. Retrieved January 13, 2002 from http://www.informationweek.com/story/IWK20010928S0005

Ford, D. P. (2003). Trust and knowledge management: The seeds of success. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 553-575). New York: Springer.

Fourth Wave Group. (2001). *Knowledge Management*. Retrieved November 28, 2002 from http://www.fourthwavegroup.com/fwg/lexicon/1592w.htm

Franz, M., Freudenthaler, K., Kameny, M., & Schoen, S. (2002). The development of the Siemens Knowledge Community Support. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 147-159). New York: Springer.

Freedom of Information Act, 5 U.S.C. § 552 (1967).

Freeman, T. (1999). Assessing innovation capacity of the consortium: An evaluation of the CAM-I cost management system program. *Journal of Knowledge Management, 3*(1), 61-65.

Friedman, M. H. (2002). Successful knowledge management initiatives rely heavily on a balance between people and technology. *Intelligent KM*. Retrieved April 16, 2001 from http://www.intelligentkm.com/feature/06/feat1.shtml

GAIN. (1996a). *Handling the obstacles to making GAIN work for you*. Retrieved July 7, 2002 from http://www.gainweb.org/

GAIN. (1996b). *The Vision of GAIN*. Retrieved July 7, 2002 from http://www.gainweb.org/

GAIN. (1996c). *What GAIN could do*. Retrieved July 7, 2002 from http://www.gainweb.org/

GAIN. (1997). *Proceedings of the Second Global Analysis and Information Network (GAIN) Conference, 27-28 May 1997*. London: The Royal Aeronautical Society.

GAIN. (1998). *Conference Summary: – Third World GAIN Conference*. Retrieved July 20, 2002 from http://www.gainweb.org/

GAIN. [2002a]. *Government Support Team*. Retrieved August 14, 2002 from http://www.gainweb.org/

GAIN. (2002b). *GAIN Action Plan, 2002-2003*. Retrieved August 4, 2003 from http://www.gainweb.org/

GAIN. (2002c). *Conference Participant Profiles*. Retrieved June 15, 2002, from http://www.gainweb.org/

GAIN. (2003a). *Sixth GAIN World Conference – Summary Report*. Retrieved August 17, 2003 from http://www.gainweb.org/

GAIN. (2003b). *Guide to automated airline safety information sharing systems*. Retrieved August 3, 2003 from http://www.gainweb.org/

GAIN. (2006a). *Previous GAIN Conferences.* Retrieved July 17, 2006 from http://www.gainweb.org/

GAIN. (2006b). *What's New in GAIN!* Retrieved April 29, 2006 from http://www.gainweb.org/

Gabbay, J., le May, A., Jefferson, H., Webb, D., Lovelock, R., Powell, J., & Lathlean, J. (2003). A case study of knowledge management in multi-agency consumer-informed 'communities of practice': Implications for evidence based policy development in health and social service. *Health*, *7*(3). 283–310.

Galipault, J. (1989, September). On communication and hazard reporting. *From Approach, the Safety Magazine of the Naval Safety Center*. Retrieved October 3, 2002 from http://www.aero-farm.com/asi/comm.htm

Galliers, B. (1999). Towards the integration of e-business, knowledge management and policy considerations within an information systems strategy framework. *The Journal of Strategic Information Systems*, *8*(3), 229-234.

Garaufis, N. (1998). *Defining the regulators role*. Retrieved July 22, 2002 from http://www.gainweb.org/

Garvey, J. F. (1998). *Remarks by the Honorable Jane F. Garvey, Administrator, Federal Aviation Administration*. Retrieved July 26, 2002 from http://www.gainweb.org/

Gellman, R. (1996). Privacy. In Hernon, P., McClure, C., & Relyea, H. (Eds.). *Federal Information Policies in the 1990s: Views and Perspectives* (pp. 137-163). Norwood, NJ: Ablex.

Germany. (1998). *Center for Social and Legal Research*. Retrieved August 23, 2003 from http://www.privacyexchange.org/legal/nat/omni/germanysum.html

Gertler, M. S., & Wolfe, D. A. (2004). Local social knowledge management: Community actors, institutions and multilevel governance in regional foresight exercises. *Futures*, *36*(1), 45-65.

Gibbert, M., Jenzowsky, S., Jonczyk, C., Thiel, M., & Völpel, S. (2002). ShareNet - the next generation: Knowledge management. In T. H. Davenport & G. J. B. Probst

(Eds.), *Knowledge Management Case Book* (2nd ed., pp. 42-59). New York: Springer.

Gibbert, M., & Krause, H. (2002). Practice exchange in a best practice marketplace. In T. H. Davenport & G. J. B. Probst (Eds.), *Knowledge Management Case Book* (2nd ed., pp. 89-107). New York: Springer.

Gillham, B. (2000). *Case Study Research Methods*. New York: Continuum.

Glaser, E. M., Abelson, H. H., & Garrison, K. N. (1983). *Putting to Use Knowledge Utilization & Implementation of Change*. San Francisco: Jossey-Bass.

Glasser, P. (1999). Knowledge mavens. *CIO*. Retrieve November 27, 2002 from http://www.cio.com/archive/enterprise/101599_book_content.html

Glazier, J. D., & Powell, R. R. (1992). *Qualitative Research in Information Management*. Englewood, CO: Libraries Unlimited.

Gloet, M., & Berrell, M. (2003). The dual paradigm nature of knowledge management: Implications for achieving quality outcomes in human resource management. *Journal of Knowledge Management*, *7*(1), 78-89.

Gormley, M. (1999, January). GAINing on safety. *Business and Commercial Aviation,* I72-73.

Gostin, L. (2000). A public health approach to reducing error: Medical malpractice as a barrier. *The Journal of the American Medical Association, 283*(13), 1742.

Gotcha. (1999). *What is Knowledge Management (KM)?* Retrieved on November 26, 2002 from University of California, Gotcha Web site: http://www.sims.berkeley.edu/courses/is213/s99/Projects/P9/web_site/about_km.html

Gottschalk, P., & Khandelwal, V. K. (2003). Determinants of knowledge management technology projects in Australian law firms. *Journal of Knowledge Management, 7*(4), 92-105.

Graham, A. B., & Pizzo, V. G. (1996). A question of balance: Case studies in strategic knowledge management. *European Management Journal*, *14*(4), 338-346.

Graham, M (2000). The threshold of the Information Age: Radio, television, and motion pictures mobilize the nation. In A. D. Chandler, & J. W. Cortada, (Eds.), *A Nation Transformed by Information* (pp. 137-176). New York: Oxford University Press.

Graham, M. (2002). *Democracy by Disclosure: the rise of technopopulism*. Washington: The Brookings Institution.

Grant, R. M. (2000). Shifts in the World Economy: The drivers of knowledge management. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 27-53). Boston: Butterworth Heinemann.

Grey, D. (1998). Knowledge management and information management: The differences. *Smith Weaver Smith*. Retrieved April 16, 2001 from http://www.smithweaversmith.com/km-im.htm

Griffith, K. S. (1998). *American Airlines Safety Action Partnership (ASAP)*. Retrieved July 14, 2002 from http://www.gainweb.org/

Gruninger, M., & Lee, J. (2002). Ontology applications and design. *Communications of the ACM*, *45*(2), 39-41.

GST. (2001a). *Reducing legal impediments to collecting and sharing safety information*. Retrieved August 23, 2002 from http://www.gainweb.org/

GST. (2001b). *Initial list of major current or planned government aviation safety information collection programs*. Retrieved August 23, 2002 from http://www.gainweb.org/

GST. (2003). *Updated list of major current or planned government aviation safety information collection programs*. Retrieved July 26, 2003 from http://www.gainweb.org/

Gupta, A. (2001). A four-faceted knowledge-based approach to surmounting borders. *Journal of Knowledge Management*, *6*(4), 291-299.

Gupta, D., Saul, M., & Gilbertson, J. (2004). Evaluation of a deidentification (De-Id) software engine to share pathology reports and clinical documents for research. *American Journal of Clinical Pathology*. *121*(6), 176-186.

Gupta, K. M. (1999). Product review Megaputer TextAnalyst. *DM Review*. Retrieved November 9, 2002 from http://dmreview.com/master.cfm?NavID=198&EdID=1478

Hahn, T. B. (2003, April/May). What has information science contributed to the world? *Bulletin of the American Society for Information Science and Technology*, *29*(4), 2-3.

Han, J., & Kamber, M. (2001). *Data Mining: Concepts and Techniques*. San Diego, CA: Academic Press.

Hara, N., Solomon, P., Kim, S.-L., & Sonnenwald, D. H. (2003). An emerging view of scientific collaboration: Scientists' perspectives on collaboration and factors that impact collaboration. *JASIST*, *54*(10), 952-965.

Hariharan, A. (2002, December). Knowledge management: A strategic tool. *Journal of Knowledge Management Practice.* Retrieve January 21, 2004 from http://www.tlainc.com/articl46.htm

Hart, C. A. (1996). *GAIN Concept Paper*. Retrieved October 30, 2000 from http://www.asy.faa.gov/gain/GAIN_information/information.htm

Hart, C. A. (1998). *What's to GAIN*. Retrieved July 14, 2002 from http://www.gainweb.org/

Hart, C. A. (2000). *Advancing the GAIN Concept*. Retrieved on July 29, 2002 from http://www.gainweb.org/

Hart, C. A. (2001). *Five short years: Reflections on GAIN's Progress*. Retrieved August 10, 2002 from http://www.gainweb.org/

Hart, C. A. (2003). *Sharing GAIN Concepts with Other Industries*. Retrieved on July 25, 2003 from http://www.gainweb.org/

Hanley, S. (1998). KM technology in the cyberorganization. *KMWorld, 7*(1). Retrieved January 18, 2002 from http://www.kmworld.com/publications/magazine/index.cfm?action=readarticle&Article_ID=402&Publication_ID=1

Helmreich, R. L. (2000). On error management: Lessons from aviation. *British Medical Journal, 320,* 781-785.

Henrotte, Jean-Pol (1997). Towards a European air safety information exchange. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 10.1-10.4). London: Royal Aeronautical Society.

Henry, N., & Pinch, S. (2000). (The) Industrial agglomeration (of Motor Sport Valley) – A knowledge, space, economy approach. In J. R. Bryson, P. W. Daniels, N. Henry, & J. Pollard (Eds.), *Knowledge, Space, Economy* (pp. 121-141). New York: Rutledge.

Herder, P. M., Veeneman, W. W., Buitenhuis, M. D. J., & Schaller, A. (2003). Follow the rainbow: A knowledge management framework for new product introduction. *Journal of Knowledge Management, 7*(3), 105-115.

Hernon, P., McClure, C. R., & Relyea, H. C. (Eds.). (1996). *Federal Information Policies in the 1990s*. Norwood, NJ: Ablex Publishing.

Hernon, P., Relyea, H. C., Dugan, R. E., & Cheverie, J. F. (2002). *United States Government Information*. Westport, CT: Libraries Unlimited.

Hibbard, J. (1998). Knowledge tools debate. *Informationweek Online*. Retrieved January 13, 2002 from http://www.informationweek.com/673/73iudeb.htm

Hildreth, P., Kimble, C., & Wright, P. (2000). Communities of practice in the distributed international environment. *Journal of Knowledge Management, 4*(1), 27-38.

Hildreth, P. M. (2004). *Going virtual: distributed communities of practice*. Hershey, PA: Idea Group Publishing.

Hinson, D. (1995). *GAIN Concept Paper: Zero Accidents*. Paper presented at the Aviation Safety Summit Progress Meeting, New Orleans, LA. Retrieved January 30, 2001 from http://www.asy.faa.gov/gain/Concepts/TEXT_OF_GAIN_CONCEPT.HTM

Hirsh, C., Youman, M., & Hanley, S. (2003). Creating knowledge-based communities of practice. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 392-413). Vienna, VA: Management Concepts.

Holsapple, C. W. (Ed.). (2003). *Handbook on Knowledge Management* (Vols. 1-2). New York: Springer.

Holsapple, C. W., & Joshi, K. D. (2002). A collaborative approach to ontology design. *Communications of the ACM, 45*(2), 42-47. Holtom, M. (1997). Global Analysis and Information Network – BASIS as a working model prototype. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 16.1-16.7). London: Royal Aeronautical Society.

Homeland Security Act of 2002, H.R. 5005, 107th Cong. (2002).

Homeland Security Information Sharing Act, H.R. 4598, 107th Cong. (2002).

Hundt, R. E. (2000). *You Say You Want a Revolution*. New Haven, CT: Yale University Press.

IATA. (2003). *STEADES*. Retrieved August 14, 2003 from http://www.iata.org/soi/safety/steades/index

Information and Command and Control. (2001). *Aerospace America*, 12, 48-49.

Institute of Safe Medication Practices. (2003). *Pharmacists, Nurses, Physicians Worldwide!* Retrieved June 14, 2003 from http://www.ismp.org/Pages/mederr_intl.html

Institute of Transportation Studies. (2000). *In May 1996, the FAA Announced a New and Innovative Approach to Reach a Goal of "Zero Accidents," Known as the Global Analysis and Information Network (GAIN).* Retrieved September 14, 2002 from University of California, Institute of Transportation Studies Web site: http://www.its.berkeley.edu/nextor/pubs/RR-98-10-abstract.html

International Atomic Energy Agency. (2003). The IAEA/NEA Incident Reporting System. *Worldatom*. Retrieved July 25, 2003 from http://www.iaea.or.at/worldatom/Press/Booklets/IaeaNea/iaeanea-irs.html

International Center for Applied Studies in Information Technology. [2001]. Glossary of knowledge management terms. *ICASIT*. Retrieved January 13, 2002 from http://www.icasit.org/km/glossary.htm

International Civil Aviation Organization. (1994, October 11). *International Standards and Recommended Practices, Aircraft Accident and Incident Investigation, Annex 13 to the Convention on International Civil Aviation*. Retrieved May 2, 2003 from http://www.icao.org/

International Civil Aviation Organization. (1999). ICAO AIG Working Paper, to Promote Information Sharing. Retrieved January 22, 2001, from http://www.gainweb.org/regulatory_issues/ICAO_AIG.htm

International Civil Aviation Organization. (2001). Resolution A33-16: ICAO Global Aviation Safety Plan (GASP). Retrieved August 17, 2003 from http://www.icao.int/icao/en/anb/meetings/anconf11/documentation/ANConf11_wp010_appb_en.pdf

Itoh, H., & Numano, M. (2002). Knowledge accumulation and sharing for cooperative environment. *In Proceedings of AIR 02: International Symposium on Artificial intelligence, Robotics, and Human-Centered Technology and Nuclear Applications, Japan,* 152-157.

Ives, W., Torrey, B., & Gordon, C. (2000). Knowledge sharing is human behavior. In D. Morey, M. Maybury, & B. Thuraisingham (Eds.), *Knowledge Management* (pp. 99-129). Cambridge, MA: The MIT Press.

Jaeger, M. (1998). *Protecting safety information in the military*. Retrieved on July 26, 2002 from http://www.gainweb.org/

Jamieson, R., & Handzic, M. (2003). A framework for security, control, and assurance of knowledge management systems. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 477-505). New York: Springer.

Japan. Information Clearinghouse. (2002). *Freedom of Information in Asia*. Retrieved September 28, 2002 from http://www.foi-asia.org/index.html

Jermola, M., Lavrač, N., & Urbančič, T. (2003). Managing business intelligence in a virtual enterprise: A case study and knowledge management lessons learned. *Journal of Intelligent & Fuzzy Systems*, *14*, 121–136.

John, R. R. (2000). Recasting the information infrastructure for the Industrial Age. In A. D. Chandler, & J. W. Cortada, (Eds.), *A Nation Transformed by Information* (pp. 55-106). New York: Oxford University Press.

Johnson, C. (2000). *Limitations of Aviation Incident Reporting*. Retrieved May 5, 2003 from University of Glasgow, Department of Computing Science Web site: http://www.dcs.gla.ac.uk/~johnson/papers/reminders

Johnson, D. B., Taira, R. K., Cardenas, A. F., & Aberle, D. R. (1997). Extracting information from free text radiology reports. *International Journal of Digital Libraries, 1,* 297-308.

Joia, L. A. (2002). Assessing unqualified in-service teacher training in Brazil using knowledge management theory: A case study. *Journal of Knowledge Management, 6*(1), 74-86.

Jurisica, I. (2000). Systematic knowledge management and knowledge discovery. *Bulletin of the American Society of Information Science, 27*(1). Retrieved November 3, 2002 from http://www.asis.org/Bulletin/Oct-00/jurisica.html

KM.Gov. (2002). *First Gov-U.S. Government*. Retrieved January 12, 2002, from http://www.km.gov/

KMWorld.com. (1999). KM -- It's even in the furniture. Retrieved January 15, 2002 from http://www.kmworld.com/resources/featurearticles/index.cfm?action=readfeature&feature_id=54

Kalnine, N. (2000). TextAnalyst supports biomedical research at CLONTECH Laboratories. *DM Review*. Retrieved November 9, 2002 from http://dmreview.com/master.cfm?NavID=198&EdID=1860

Kelly, T. M., & Bauer, D. K. (2003). Managing intellectual capital - via E-Learning - at Cisco. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 511-532). New York: Springer.

Kenney, M. (2000). Introduction. In M. Kenney (Ed.), *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region* (pp. 1-12). Palo Alto, CA: Stanford University Press.

Kidwell, J. J., Linde, K. M. V., & Johnson, S. L. (2000). Applying corporate knowledge management practices in higher education. In G. Bernbom (Ed.), *Information Alchemy: The Art and Science of Knowledge Management* (pp. 1-24). San Francisco: Jossey-Bass.

Kim, M. P. (2003). Organizational readiness for knowledge management. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 127-154). Vienna, VA: Management Concepts.

Kirk, J., & Miller, M. L. (1987). *Reliability and Validity in Qualitative Research*. London: Sage.

Klaaran, J. (2003). *Access to Information and National Security in South Africa*. Maxwell Campbell Public Affairs Institute. Retrieved July 14, 2003 from http://www.maxwell.syr.edu/campbell/opengov/Klaaren.pdf

Koenig, M. E. D. (2004). Knowledge management and research on research: What has been learned? In M. E. D. Koenig & T. K. Srikantaiah (Eds.), *Knowledge Management Lessons Learned* (pp. 113-120). Medford, NJ: ASIS.

Koenig, M. E. D., & Srikantaiah, T. K. (2000). The evolution of knowledge management. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 23-36). Medford, NJ: ASIS.

Kolczynski, P. J. (1998). *FOQA - Aviation Safety V. Legal Rights*. Retrieved July 17, 2002 from http://www.aviationlawcorp.com/content/foqasafety.htm#DISCOVERY%20OF%20FOQA%20DATA%20IN%20CIVIL

Krebs, B. (2002). Critics blast IT loophole in Homeland Security plan. *Washingtonpost.com*. Retrieved July 27, 2002 from http://www.washingtonpost.com/wp-dyn/articles/A58311-2002Jul24.html

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology*. London: Sage.

Krogh, G. V., Ichijo, K., & Nonaka, I. (2000). *Enabling Knowledge Creation*. New York: Oxford University Press.

Kurzweil, R. (1999). *The Age of Spiritual Machines*. New York: Viking.

Kvale, S. (1996). *Interviews*. London: Sage.

Ladd, A., & Ward, M. A. (2002, August). An investigation of environmental factors influencing knowledge transfer. *Journal of Knowledge Management Practice*. Retrieved January 28, 2004 from http://www.tlainc.com/

Lamont, J. (2006, July/August). Transportation: Communities of practice leverage knowledge. *KMWorld*, 14-15.

Lasky, B., & Tare, M. (2002). Knowledge management: A 21st century role for the human resource professional (Swinburne University of Technology). Paper presented at the meeting of IFSAM 2002 Conference, Gold Coast, Queensland, Australia. Retrieved January 26, 2005 from http://www.ifsam.org/2002/Lasky&Tare.pdf

Lebow, C. C., Sarsfield, L. P., Stanley, W. L., Ettedgui, E., & Henning, G. (1999). *Safety in the Skies.* Santa Monica, CA: Rand Institute for Civil Justice.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical Knowledge* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall.

Lebow, C. C., Sarsfield, L. P., Stanley, W. L., Ettedgui, E., & Henning, G. (1999). *Safety in the Skies.* Santa Monica, CA: Rand Institute for Civil Justice.

Leroy, G., & Chen, H. (2005). Genescene: An ontology-enhanced integration of linguistic and co-occurrence based relations in biomedical texts. *JASIST*, *56*(5), 457-468.

Lesser, E. L., Fonyaine, M. A., & Slusher, J. A. (2000). *Knowledge and Communities.* Boston: Butterworth Heinemann.

Lesser, E., & Prusak, L. (2000). Communities of practice, social capital and organizational knowledge. In E. l. Lesser, M. A. Fontaine, & J. A. Slusher (Eds.), *Knowledge and Communities* (pp. 123-131). Boston: Butterworth Heinemann.

Levett, G. P., & Guenov, M. D. (2000). A methodology for knowledge management implementation. *Journal of Knowledge Management, 4*(3), 258-269.

Liddy, E. D. (2000). Text-mining. *Bulletin of the American Society for Information Science, 27*(1). Retrieved October 27, 2002 from http://www.asis.org/Bulletin/Oct-00/liddy.html

Lloyd, B. (1996). Knowledge management: The key to long-term organizational success. *Long Range Planning*, *29*(4), 576-580.

Logan, T. (1998). *Benefits of Operational Safety Information*. Retrieved July 14, 2002 from http://www.gainweb.org/

Logan, T., & Ananyan, S. (2003). *Application of PolyAnalyst at Southwest Airlines*. Retrieved September 19, 2003 from http://www.gainweb.org/

Lopez, X. (1998). *The Dissemination of Spatial Data*. London: Ablex.

Lovelace, H. W. (1999). Ask the secret CIO. *Informationweek Online.* Retrieved January 13, 2002 from http://www.informationweek.com/719/secret.htm

Lubar, S. D. (1993). *Infoculture*. Boston: Houghton Mifflin Company.

Lynch, D. J. (2002). Business versus terror. *Foreign Policy*. Retrieved June 29, 2003 from http://www.foreignpolicy.com/issue_mayjune_2002/rothkopf.html

Machlup, F., & Mansfield, U. (Eds.). (1983). *The Study of Information: Interdisciplinary Messages*. New York: Wiley.

Macintosh, A., Filby, I., & Kingston, J. (1999). Knowledge management techniques: Teaching and dissemination concepts. *International Journal of Human-Computer Studies*, *51*(3), 549-566.

Magg, G. D., & Flint, J. A. (2004). The role of corporate intelligence gathering in the modern business decision-making environment. In E. D. Koenig & T. K. Srikantaiah, (Eds.), *Knowledge Management Lessons Learned* (pp. 403-440). Medford, NJ: Information Today.

Maier, R., Hädrich, T., & Peinl, R. (2006). *Enterprise Knowledge Infrastructures*. New York: Springer.

Malecki, E. J. (2000). Competitiveness: Local knowledge and economic geography. In J. R. Bryson, P. W. Daniels, N. Henry, & J. Pollard (Eds.) *Knowledge, Space, Economy*, 103-119. New York: Rutledge.

Malhotra, Y (2000). From information management to knowledge management: Beyond the "high-tech hidebound systems." In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 37-61). Medford, NJ: ASIS.

Malhotra, Y. (2001). Knowledge management for the new world of business. *Brint.Com*. Retrieved January 13, 2002 from http://www.brint.com/km/whatis.htm

Management practices vary widely among airlines. (2002). *AirSafety Week, 16*(4). Retrieved August 30, 2003 from http://web.lexis-nexis.com

Mancini, L. (1998). *Conference Summary of the Third GAIN World Conference, November 3-5, 1998, Long Beach, California*. Retrieved July 14, 2002 from http://www.gainweb.org/

Marakas, G. M. (2002). *Modern Data Warehousing, Mining, and Visualization*. Upper Saddle River, NJ: Prentice Hall.

March, J. (1997). Information politics. In T. H. Davenport (Ed.), *Information Ecology*, (pp. 67-82). New York: Oxford University Press.

Marett, P. (2002). *Information Law in Practice*, (2nd ed.). Burlington, VT: Ashgate.

Martin, B. (2003). *Whistleblowing and Suppression of Dissent*. Retrieved July 14, 2003 from University of Wollongong, Brian Martin Web site: http://www.uow.edu.au/arts/sts/bmartin/dissent/

Marwick, A. D. (2001). Knowledge management technology. *IBM Systems Journal, 40*(4). Retrieved January 15, 2002 from http://www.research.ibm.com/journal/sj/404/marwick.html

Mason, D., & Pauleen, D. (2003). Perceptions of knowledge management: A qualitative analysis. *Journal of Knowledge Management, 7*(4), 38-48.

Mason, J. (2002). *Qualitative Researching* (2nd ed.). London: Sage.

Matthews, S. (1998, November). *Freedom and an Open Society – Roadblocks to Improving Aviation Safety in the U.S.A.* Paper presented at the meeting of the Third GAIN World Conference, Long Beach, California.

Mattison, R. (1999). *Web Warehousing and Knowledge Management*. New York: McGraw-Hill.

McCarthy, P. (1998, November). *Data Protection Under ICAO Annex 13 – A Proposal*. Paper presented at the meeting of the Third GAIN World Conference, Long Beach, California.

McCarthy, P. (2000, June). *Reducing Impediments (Organizational, Regulatory, Civil Litigation, Criminal Sanction, Risk of Public Disclosure)* – Working Group D. Paper presented at the meeting of the Fourth GAIN World Conference, Paris, France.

McClure, C. R., & Ryan, J. (1996). Moving to the networked information environment: New challenges and issues. In P. Hernon, C. R. McClure, & H. C. Relyea, (Eds.), *Federal Information Policies in the 1990s* (pp. 297-313). Norwood, NJ: Ablex Publishing.

McConnachie, G. (1997). The management of intellectual assets: Delivering value to the business. *Journal of Knowledge Management, 1*(1), 56-62.

McElroy, M. W. (2003). *The New Knowledge Management*. New York: Butterworth Heinemann.

McInerney, C. (2002). Knowledge management – A practice still defining itself. *Bulletin of the American Society for Information Science and Technology*, *28*(3), 14-15.

Meadow, C. T. (1992). *Text Information Retrieval Systems*. New York: Academic Press.

Megaputer. (2003). *TextAnalyst 2 User Manual*. Retrieved June 25, 2004 from http://www.megaputer.com/

Mena, J. (2003*). Investigative Data Mining for Security and Criminal Detection*. Boston: Butterworth-Heinemann.

Mendel, T. (2003). *National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles*. Campbell Public Affairs Institute. Retrieved June 29, 2003 from http://www.maxwell.syr.edu/campbell/opengov/index.html

Moffett, S., McAdam, R., & Parkinson, S. (2003). An empirical analysis of knowledge management applications. *Journal of Knowledge Management*, *7*(3), 6-26.

Morey, D., Maybury, M., & Thuraisingham, B. (Eds.). (2000). *Knowledge Management*. Cambridge, MA: The MIT Press.

Muralidar, S. (2000). Knowledge management: A research scientist's perspective. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 221-232). Medford, NJ: ASIS.

Murphy, T. (1997). Perspectives on GAIN. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 13.1-13.5). London: Royal Aeronautical Society.

Murray, P. (2000). Designing business benefits for knowledge management. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 171-194). Boston: Butterworth Heinemann.

Murty, K. S. [2003]. Role of HR in institutionalizing knowledge management in a company. *Association of Knowlegework*. Retrieved October 25, 2003 from http://www.kwork.org/White%20Papers/hr-km.html

Na Ubon, A., & Kimble, C. (2002). Knowledge management in online distance education. *Proceedings of the 3rd International Conference Networked Learning 2002*, *University of Sheffield*, *UK*, *March*, 465-473.

Nardi, B. A., & O'Day, V. L. (1999). *Information Ecologies: Using Information with Heart*. Cambridge, MA: The MIT Press.

Neuendorf, K. A. (2002). *The Content Analysis Guidebook*. London: Sage.

New Zealand. [2003]. Official information: Your right to know. *Govt.nz*. Retrieved July 14, 2003 from http://www.justice.govt.nz/pubs/other/pamphlets/2001/info_act.html

Newell, S., Robertson, M., & Swan, J. (2006). Interactive innovation processes and the problems of managing knowledge. In B. Renzl, K. Matzler, & H. Hinterhuber, (Eds.), *The Future of Knowledge Management* (pp. 115-136). New York: Palgrave Macmillan.

Nielsen, B. B. (in press). The role of knowledge embeddedness in the creation of synergies in strategic alliances. *Journal of Business Research*.

Nonaka, I., & Reinmoeller, P. (2000). Dynamic business systems for knowledge creation and utilization. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 89-112). Boston: Butterworth Heinemann.

O'Dell, C., & Grayson, C. J. (1998). *If We Only Knew What We Know*. New York: The Free Press.

O'Dell, C., Hasanali, F., Hubert, C., Lopez, K., Odem, P., & Raybourn, C. (2003). Successful KM implementations: A study of best-practice organizations. . In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 411-441). New York: Springer.

O'Leary, M. (2002). The British Airways human factors reporting programme. *Reliability Engineering & System Safety*, *75*, 245-255.

Oncology Nursing Society. (2002). Prevention and Reporting of Medication Errors. Retrieved on May 17, 2006 from http://www.ons.org/publications/positions/MedicationErrors.shtml

Orlady, H. W., & Orlady, L. M. (1999). *Human factors in Multi-Crew Flight Operations*. Brookfield, VT: Ashgate.

Paller, A. (2002). Testimony of Alan Paller, Director of Research, SANS Institute. *Before the Committee on Government Affairs, United States Senate Hearing on Securing Our Infrastructure: Private/Public Information Sharing*. Retrieved on July 27, 2002 from http://www.senate.gov/~gov_affairs/050802paller.pdf

Pan, S. L., & Leidner, D. E. (2003). Bridging communities of practice with information technology in pursuit of global knowledge sharing. *The Journal of Strategic Information Systems*, *12*(1), 71-88.

Pan, S. L., & Scarbrough, H. (1998). A socio-technical view of knowledge sharing at Buckman Laboratories. *Journal of Knowledge Management, 2*(1), 55-66.

Patient Safety Reporting System. (2003). *PSRS Program Overview*. Retrieved on June 21, 2003 from http://psrs.arc.nasa.gov/

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods* (3rd ed.). London: Sage.

Peña, I. (2002). Knowledge networks as part of an integrated knowledge management approach. *Journal of Knowledge Management*, *6*(5), 469-478. Peña, I. (2002). Knowledge networks as part of an integrated knowledge management approach. *Journal of Knowledge Management, 6*(5), 469-478.

Pereira, R. C. C. (2002). Facilitating the exchange of safety-related information. *ICAO*. Retrieved August 17, 2003 from http://www.gainweb.org/

Pinelli, T. E., Barclay, R. O., & Kennedy J. M. (1996). U.S. scientific and technical information policy. In P. Hernon, C. R. McClure, & H. C. Relyea, (Eds.), *Federal Information Policies in the 1990s* (pp. 211-232). Norwood, NJ: Ablex Publishing

Pinelli, T. E., Barclay, R. O., Kennedy, J. M., & Bishop, A. P. (Eds.). (1997). *Knowledge Diffusion in the U.S. Aerospace Industry: Managing Knowledge for a Competitive Advantage (Parts A-B).* Greenwich, CT: Ablex Publishing.

Pinker, S. (1997). *How the Mind Works*. New York: Norton.

Platt, N. (2000). Knowledge management: Can it exist in a law office? In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 405-416). Medford, NJ: ASIS.

Ponzi, L. J. (2004). Knowledge management: Birth of a discipline. In E. D. Koenig & T. K. Srikantaiah, (Eds.), *Knowledge Management Lessons Learned* (pp. 9-26). Medford, NJ: Information Today.

Popping, R. (2000). *Computer-assisted Text Analysis*. London: Sage.

Posluns, H. (2001). Global information sharing systems. In *Safety Information Sharing; Collaboration, Innovation, Implementation*. Symposium Conducted at the Fifth GAIN World Conference, Miami, FL.

Posluns, H. (2003). *Overview of automated airline safety information sharing systems*. Retrieved August 14, 2003 from http://www.gainweb.org/

Post, W. (2002). *ECCAIRS: A Network for Aviation Occurrence Information*. Paper presented at the April 12, 2002 International Conference of the Italian Flight Safety Committee. Retrieved August 24, 2002 from http://www.italianflightsafetycommittee.org/ftp/varie/convegno-aprile02/Svt/15.pdf

Potter, S. (2001, November/December). Building an enterprise taxonomy [Special supplement]. *KMWorld*, 15.

Predmore, S. (2003). *GAIN's Seventh Birthday -- What Has Our Collaboration Achieved*. Retrieved August 3, 2003 from http://www.gainweb.org/

Predmore, S. (2001). GAIN update and conference perspective. In *Safety Information Sharing; Collaboration, Innovation, Implementation*. Symposium conducted at the Fifth GAIN World Conference, Miami, FL.

Privacy Act of 1974, 5 U.S.C. § 552a (1974).

Prusak, L. (2001). Where did knowledge management come from? *IBM Systems Journal, 40*(4), 1002-1007.

Qin, J. (2000). Working with data: Discovering knowledge through mining and analysis. *Bulletin of the American Society for Information Science, 27*(1). Retrieved March 7, 2003 from http://www.asis.org/Bulletin/Oct-00/qin.html

Ranter, H. (2001). *Access to Air Safety Information*. Paper presented at the 8th Annual MRO Regulations, Quality and Safety Conference. Retrieved September 21, 2002 from http://aviation-safety.net/pubs/Access-ASI-paper.pdf

Rayward, W. B. (1998).The history and historiography of information science: Some reflections. In T. B. Hahn & M. Buckland, (Eds.). *Historical Studies in Information Science* (pp. 7-21).Medford, NJ: ASIS.

Reason, J. (1997). Corporate culture and safety. *NTSB Symposium on Corporate Culture and Transportation Safety*. Washington: April 1997.

Relyea, H. C. (1996). Freedom of information revisited. In P. Hernon, C. McClure, & H. Relyea, (Eds.). *Federal Information Policies in the 1990s: Views and Perspectives* (pp. 183-210). Norwood, NJ: Ablex.

Remez, S. G. (2003a). Who will lead the Knowledge Revolution? In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 285-300). Vienna, VA: Management Concepts.

Remez, S. G. (2003b). KM and E-Gov. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp. 207-223). Vienna, VA: Management Concepts.

Remez, S. G., & Desenberg, J. M. (2003). Information technology and knowledge management: The medium and the message. In R. C. Barquin, A. Bennet, & S. G. Remez, (Eds.), *Knowledge Management: The Catalyst for Electronic Government* (pp.155-177). Vienna, VA: Management Concepts.

Reno, J. (1993, October 4). *Memorandum for Heads of Departments and Agencies: The Freedom of Information Act.* Retrieved May 10, 2003 from http://www.fas.org/sgp/clinton/reno.html

Repeta, L., & Schultz, D. M. (2002). Japanese government information: New rules for access. *The National Security Archive*. Retrieved July 14, 2003 from http://www.gwu.edu/~nsarchiv/nsa/foia/japanfoia.html

Report of the Committee on Commerce, Science, and Transportation on S. 342, Senate, 106th Cong. (1999). Retrieved December 22, 2005 from the Library of Congress database.

Restoration of Freedom of Information Act of 2003, S. 609, 108th Cong. (2003).

Rifkin, J. (2000). *The Age of Access*. New York: Tarcher Putnam.

Roberts, P. R. (2001). ASMS submission to Dr Parry inquiry. *Scoop*. Retrieved August 17, 2002 from http://www.scoop.co.nz/mason/stories/PO0112/S00023.htm

Robertson, S. (2002). A tale of two knowledge-sharing systems. *Journal of Knowledge Management*, *6*(3), 295-308.

Rolland, N., & Chauvel, D. (2000). Knowledge transfer in strategic alliances. In C. Despres, & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 225-236). Boston: Butterworth Heinemann.

Rosenthal, L. (2002). *Aviation Safety and Reporting System*. Retrieved September 28, 2002 from http://www.battelle.org/transportation/solutions.stm#AvSafety

Roth, J. (2003). Enabling knowledge creation: Learning from an R&D organization. *Journal of Knowledge Management, 7*(1), 32-48.

Rothenburger, B., & Galarreta, D. (2006). Facing knowledge evolution in space project: a multi-viewpoint approach. *Journal of Knowledge Management, 10*(2), 52-65.

Rothkopf, T. (2002). Breaking the vicious cycle: Preserving our liberties while fighting terrorism. *Cato Policy Analysis, 443*, 2-21.

Rubenstein-Montano, B., Buchwalter, J., & Liebowitz, J. (2001). Knowledge management: A U.S. Social Security Administration case study. *Government Information Quarterly, 18*(3), 223-253.

Ryske, E. J., & Sebastian, T. B. (2000). From library to knowledge center: The evolution of a technology infocenter. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 389-402). Medford, NJ: ASIS.

Safe Medical Act of 1990, 21st Cong., §301-394 (1990).

Sahasrabudhe, V. (2000). Information technology in support of knowledge management. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management for the Information Professional* (pp. 269-276). Medford, NJ: ASIS.

Saint-Onge, H. (1996). *Tacit Knowledge: The Key to the Strategic Alignment of Intellectual Capital*. Retrieved June 9, 2004, from http://www.konvergeandknow.com/articles/tacitknow.html

Salisbury, M. W. (2003). Putting theory into practice to build knowledge management systems. *Journal of Knowledge Management*, *7*(2), 128-141.

San Diego State University. (1999). *What is Knowledge Management?* Retrieved January 13, 2002 from San Diego University, Knowledge Management Web site: http://defcon.sdsu.edu/1/objects/km/defining/index.htm

Sanchez, R. (2006). Knowledge management and organizational learning: Fundamental concepts for theory and practice. In B. Renzl, K. Matzler, & H. Hinterhuber, (Eds.), *The Future of Knowledge Management* (pp. 29-61). New York: Palgrave Macmillan.

Saris-Gallhofer, I. N., Saris, W. E., & Morton, E. L. (1978). A validation study of Holsti's Content Analysis Procedure. *Quality and Quantity, 12*, 131-145.

Sawyer, S., Eschenfelder, K., & Heckman, R. (2000). Knowledge markets: Cooperation among distributed technical specialist. In T. K. Srikantaiah & M. E.D. Koenig (Eds.), *Knowledge Management* (pp. 181-204). Medford, NJ: ASIS.

Sayce, A. (2001). Legal impediments to safety information collection and sharing. In *Safety Information Sharing; Collaboration, Innovation, Implementation*. Symposium conducted at the Fifth GAIN World Conference, Miami, FL.

Schreckengast, S. (1997). Aviation safety data sources. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 17.1-17.7). London: Royal Aeronautical Society.

Schrimer, A. L. (2003). Privacy and knowledge management: Challenges in the design of the Lotus Discovery Server. *IBM Systems Journal, 42*(3), 51-53.

Schröder, H.-H. (2006). Wrapping is all up – past, present, and future of knowledge integration. In A. Jetter, J. Kraaijenbrink, H.-H. Schröder, & F. Wijnhoven, (Eds.), *Knowledge Integration* (pp. 175-191). Heidelberg, Germany: Physica-Verlag.

Shein, E. (2003). Homeland Security CIO: Information (sharing) is power. *BetterManagment.com.* Retrieved June 29, 2003 from http://www.bettermanagement.com/Library/Library.aspx?a=8&LibraryID=5103

Shapiro, C., & Varian, H. R. (1999). *Information Rules*. Boston: Harvard Business School Press.

Sieloff, C. G. (1999). "If only HP knew what HP knows": The roots of knowledge management at Hewlett-Packard. *Journal of Knowledge Management, 3*(1), 47-53.

Simmons, J. L., & Forrest, J. S. (2005). United States aviation safety data: uses and issues related to sanctions and confidentiality. *Journal of Air Law & Commerce*. *70*(1). 83-112.

Sinclair, N. (2006). *Stealth KM*. New York: Butterworth-Heinemann.

Skyrme, D. J. (2000). Developing a knowledge strategy: From management to leadership. In D. Morey, M. Maybury, & B. Thuraisingham (Eds.), *Knowledge Management* (pp. 61-83).Cambridge, MA: MIT Press.

Smith, D. E. (2000). Knowledge, groupware and the Internet. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 393-407). New York: Springer.

Smith, H. A., & McKeen, J. D. (2003a). *Creating and Facilitating Communities of Practice*. Retrieved July 4, 2004 from Queen's University Web site: http://business.queensu.ca/kbe/docs/Smith-McKeen%2003-09.pdf

Smith, H. A., & McKeen, J. D. (2003b). Knowledge management in organizations: The state of current practice. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 395-410). New York: Springer.

Snowden, D. (2000). The social ecology of knowledge management. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 237-265). Boston: Butterworth Heinemann.

Snyder, W. M. (1997). Communities of practice: Combining organizational learning and strategy insights to create a bridge to the 21st century. *Community Intelligence Labs*. Retrieved June 20, 2002 from http://www.co-i-l.com/coil/knowledge-garden/cop/cols.shtml

Spender, J. –C. (2000). Managing knowledge systems. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 149-167). Boston: Butterworth Heinemann.

SRG. [2001]. *Safety Data*. Retrieved September 28, 2002 from http://www.caa.co.uk/srg/safety_initiatives/default.asp?page=8

Srikantaiah, T. K. (2000). Knowledge management: A faceted overview. In T. K. Srikantaiah & M. E. D. Koenig (Eds.), *Knowledge Management* (pp. 1-17). Medford, NJ: ASIS.

Srikantaiah, T. K., & Koenig, M. E. D. (2000). *Knowledge Management*. Medford, NJ: ASIS.

Stake, R. E. (1995). *The Art of Case Study Research*. Thousand Oaks, CA: Sage.

Standage, T. (1998). *The Victorian Internet*. New York: Walker & Co.

Starbuck, W. H. (1997). Learning by knowledge-intensive firms. In L. Prusak (Ed.), *Knowledge in Organizations* (pp. 147-175). Boston: Butterworth Heinemann.

Steinke, S. [2002]. European Confidential Aviation Safety Reporting Network will close! *EUCARE*. Retrieved August 26, 2002 from http://www.eucare.de/end.htm

Stevens, L. (2000). Incentives for sharing. *Knowledge Management*, *3*(10), 54-60.

Stewart, T. A. (2001). *The Wealth of Knowledge*. New York: Currency.

Stewart, T. A. (2002). The case against knowledge management. *Business2.0*. Retrieved January 13, 2002, from http://www.business2.com/articles/mag/print/0,1643,36747,FF.html

Strassmann, P. A. (1995). *The Politics of Information Management*. New Canann, CT: The Information Economic Press.

Strassmann, P. A. (1999). Does knowledge capital explain market/book valuations? *Freedom Technology Media Group*. Retrieved June 18, 2001, from http://www.straussmann.com

Sullivan, C. (2001). *Who cares about CAIR?* Retrieved August 29, 2004 from http://www.asasi.org/papers/2001/Who%20Cares%20About%20CAIR.pdf

Sullivan, D. (2001). *Document Warehousing and Text Mining*. New York: Wiley.

Sveiby, K. E. (2001). *Knowledge management – Lessons from the pioneers*. Retrieved January 29, 2002, from http://sveiby.konverge.com/library.html

Swan, J. (2003). Knowledge management in action? In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 271-296). New York: Springer.

Swan, J., & Scarbrough, H. (2001). Knowledge, purpose, and process: Linking knowledge management and innovation. *Proceedings presented at the 34th Hawaii International Conference on System Sciences*.

Swan, J., & Scarbough, H. (2002). The paradox of “knowledge management.” *Upgrade, 3*(1). Retrieved June 9, 2002, from http://www.upgrade-cepis.org/issues/2002/1/upgrade-vIII-1.pdf

Takahashi, T., & Vandenbrink, D. (2004). Formative knowledge: From knowledge dichotomy to knowledge geography - knowledge management transformed by the ubiquitous information society. *Journal of Knowledge Management, 8*(1), 64-76.

Tamuz, M. (1997). De-identification: Promoting the exchange of GAIN data while protecting the identity of data sources. *Global Analysis and Information Network (GAIN) Proceedings* (pp. 8.1-8.21). London: Royal Aeronautical Society.

Tapscott, D. (1996). *The Digital Economy*. New York: McGraw Hill.

Temin, T. R. (2004). Taking data to a higher plane. *GCN*. Retrieved September 3, 2004 from http://www.gcn.com

Thomas, J. C., Kellogg, W. A., & Erickson, T. (2001). The knowledge management puzzle: Human and social factors in knowledge management. *IBM Systems Journal, 40*(1). Retrieved January 18, 2002 from http://www.research.ibm.com/journal/sj/404/thomas.html

Turban, E., McLean, E., & Wetherbe, J. (2002). *Information Technology for Management*. New York: Wiley.

U.K. Civil Aviation Authority. (1991). *Statutory Instrument No. 1672*. Retrieved September 28, 2002 from http://www.hmso.gov.uk/si/si1991/Uksi_19911672_en_3.htm

U.S. Chief Information Officers Council. (2003). *Statement of Mark Forman before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census (data mining testimony) March 25, 2003*. Retrieved September 20, 2003 from http://www.cio.gov/documents/testimony_forman_3_25_03.html

U.S. Department of Justice. (2002). *Freedom of Information Act*. Retrieved July 16, 2002 from http://www.usdoj.gov/oip/foi-act.htm

U.S. Department of Transportation. (1998). *White House Commission on Aviation Safety and Security – The DOT Status Report*. Retrieved February 16, 2003 from http://www.dot.gov/affairs/whcsec1.htm

U.S. Department of Transportation. [2002]. *Aviation Safety Data*. Retrieved September 22, 2002 from http://www.bts.gov/ntda/sdfaa/desc.html

U.S. F.A.A. (2000a). *Overview of First Global Analysis and Information Network (GAIN) Workshop*. Retrieved October 13, from http://www.asy.faa.gov/gain/Conferences/GAIN/wkshpsum.htm

U.S. F.A.A. (2000b). *Overview of Second Global Analysis and Information Network Conference*. Retrieved October 13, 2000 from http://www.asy.faa.gov/gain/Conferences/GAIN2/intro.htm

U.S. F.A.A. (2000c). *Using Information Proactively to Improve Aviation Safety*. Retrieved October 13, 2000 from http://www.asy.faa.gov/gain/GAIN_information/information.htm

U.S. F.A.A. (2000d). *Aviation Safety Action Programs (ASAP)*. (AC No. 120-66A). Washington: Government Printing Office.

U.S. F.A.A. (2000e). *Aviation Safety Action Programs (ASAP)*. (AC No. 120-66B). Washington: Government Printing Office.

U.S. F.A.A. Flight Standards Service. (2003). Service Difficulty Reporting. *Av-info.FAA.gov*. Retrieved July 27, 2003 from http://av-info.faa.gov/isdr/

U.S. F.A.A. National Civil Aviation Review Commission. (1997). *Avoiding Aviation Gridlock & Reducing the Accident Rate*. Retrieved August 29, 2003 from http://www1.faa.gov/NCARC

U.S. F.A.A. Office of Aerospace Medicine. (1999). *The Role of Shift Work and Fatigue in Air Traffic Control Operational Errors and Incidents*. Retrieved September 14, 2002 from http://www.cami.jccbi.gov/AAM-400A/Abstracts/1999/am99-02.html

U.S. F.A.A. Office of System Safety. (1997). *Safety Reports*. Retrieved July 25, 2003 from http://www.nasdac.faa.gov/aviation_studies/safety_data/safety_data_index.html

U.S. F.A.A. Office of System Safety. (2002). *The Global Aviation Information Network (GAIN): Using Information Proactively to Improve Aviation Safety*. Retrieved May 30, 2002 from http://www.gainweb.org/

U.S. F.A.A. Office of System Safety. (2003). *How to Report a Safety Problem*. Retrieved July 27, 2003 from http://www.asy.faa.gov/asy_internet/safetyhotline.htm

U.S. Federal Highway Administration. (1997). Knowledge Sharing Success Story: Rumble Strips Government-to-Government Community of Practice. *KM Gov*. Retrieved June 20, 2002 from http://www.km.gov/stories/FHWA_Rumble-Strips.doc

U.S. Fire Administration. (2003). *National Fire Incident Reporting System*. Retrieved July 25, 2003 from http://www.usfa.fema.gov/inside-usfa/nfirs2.shtm

U.S. National Aeronautics and Space Administration. (2000). *The ASRS Program Briefing*. Retrieved September 28, 2002 from http://asrs.arc.nasa.gov/briefing/program_briefing.htm

U.S. National Civil Aviation Review Commission. (1997). *Avoiding Aviation Gridlock and Reducing the Accident Rate*. Retrieved May 16, 2006 from http://www.aerostates.org/ASA_files/NCARCSummary.pdf

U.S. National Transportation Safety Board (2002). *Answers to Frequently Asked Questions about FOIA*. Retrieved July 20, 2002, from http://www.ntsb.gov/info/foia.htm

U.S. National Transportation Safety Board Part 830, 49 C.F.R. § 830.2 (Oct. 24, 1988).

U.S. Occupational Safety and Health Administration. (2002). *Agreement Establishing an Alliance Between the Occupational Safety and Health Administration U.S. Department of Labor and the American Biological Safety Association*. Retrieved July 25, 2003 from http://www.osha.gov/dcsp/alliances/absa/absa_final_9-23-02.pdf

U.S. Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Retrieved June 28, 2003 from http://www.whitehouse.gov/homeland/book/

U.S. Office of Management and Budget. (2003). *H.R. 4598 – Homeland Security Information Sharing Act*. Retrieved June 29, 2003 from http://www.whitehouse.gov/omb/legislative/sap/107-2/HR4598-h.html

USA Patriot Act, H.R. 3162, 147th Cong. (2001).

UNESCO-IHE Institute for Water Education. (2003). *Text-Mining for Knowledge Management*. Retrieved September 19, 2003 from http://www.ihe.nl/vmp/articles/Projects/PRO-NL_TMining.html

United Nations. (1948). *Universal Declaration of Human Rights*. Retrieved July 3, 2003 from http://www.un.org/Overview/rights.html

University of Texas. [2001]. *Knowledge Management Glossary*. Retrieved January 13, 2002 from University of Texas, KM Web site: http://www.bus.utexas.edu/kman/glossary.htm

University of Toronto. (2000). *Your Knowledge @ Work*. Retrieved January 13, 2002 from University of Toronto, Knowledge Management Initiatives Web site: http://www.fis.utoronto.ca/kmi/index.htm

Uribe, C. L., Schweikhart, S. B., Pathak, D. S., Dow, M., & Marsh, G. B. (2002). Perceived barriers to medical-error reporting: An exploratory investigation. *Journal of Healthcare Management, 47*(4), 263-281.

van der Spek, R., Hofer-Alfeisa, J., & Kingma, J. (2003). The knowledge strategy process. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 443-466). New York: Springer.

Varian, H. R., & Shapiro, C. (1999). *Information Rules*. Boston: Harvard Business School Press.

Venkata, R. (2002, October). Taxonomies, categorization, and organizational agility. *KMWorld*, (Suppl.), S12-S13.

Verton, D. (2003). Progress on info-sharing threatened by changes to FOIA law. *Computerworld*. Retrieved May 11, 2003 from http://www.idg.net/ic_1231647_9720_1-5073.html

Veterans' Benefits Act, 38 U.S.C. § 5705 (1997).

Vickery, B. C., & Vickery, A. (1987). *Information Science in Theory and Practice*. London: Butterworths.

von Krogh, G. (2001). The communal resource and information systems. *The Journal of Strategic Information Systems*, *11*(2), 85-107.

Voss. B. D. (2001). Knowledge management alleviates the computing support crisis at Indiana University. In G. Bernbom (Ed.), *Information Alchemy: The Art and Science of Knowledge Management* (pp. 99-113). San Francisco: Jossey-Bass.

Wadham, J., & Modi, K. (2003). *National Security and Open Government in the United Kingdom*. Retrieved July 4, 2003 from http://www.maxwell.syr.edu/campbell/opengov/Wadham.pdf

Wagner, B. A. (2003). Learning and knowledge transfer in partnering: An empirical case study. *Journal of Knowledge Management, 7*(2), 97-113.

Ward, K. (2001). *The Pursuit of Professionalism*. Retrieved August 17, 2002 from CAA, Australasian University Aviation Association 2001 Conference, Massey University School of Aviation Web site: http://www.caa.govt.nz/publicinfo/DCA_speech_AUAA.htm

Warwick University. Business Processes Resource Centre. [2001]. *Defining Knowledge Management*. Retrieved January 13, 2002 from Warwick University, BPRC Web site: http://bprc.warwick.ac.uk/Kmweb.html#SEC1

Wei, C.-P., Piramuthu, S., & Shaw, M. J. (2003). Knowledge discovery and data mining. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 157-189). New York: Springer.

Weinberger, D. (2001). Let me count the KM ways. *KMWorld*. Retrieved January 18, 2002 from http://www.kmworld.com/resources/featurearticles/index.cfm?action=readfeature&feature_id=8

Weir, S. (2002). Promises, promises: An audit of new Labour's record reveals a democratic deficit at the heart of government. *New Statesman, 131*(4610), p. 28.

Weiser, M., Gold, R., & Brown, J. S. (1999). The origins of ubiquitous computing at PARC in the late 1980s. *IBM Systems Journal*, *38*(4), 693-696.

Weiss, S. M., Apte, C., Damerau, F. J., Johnson, D. E., Oles, F. J., Goetz, T., & Hampp, T. (1999). Maximizing text-mining performance. *IEEE*. Retrieved June 28, 2004 from http://www.research.ibm.com/dar/papers/pdf/ieee99_mtmp.pdf

Wells, A. T. (2001). *Commercial Aviation Safety* (3rd ed.). New York: McGraw-Hill.

Wenger, E. (1998). *Communities of Practice: learning, meaning, and identity*. Cambridge, UK: Cambridge University Press.

Wenger, E. (2000). Communities of practice: The structure of knowledge stewarding. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 205-224). Boston: Butterworth Heinemann.

Wenger, E., McDermott, R., & Snyder, W. M. (2002). *Cultivating Communities of Practice*. Boston: Harvard Business School Press.

Wensley A. K. P., & Verwijk-O' Sullivan, A. (2000). Tools for knowledge management. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp.113-147). Boston: Butterworth Heinemann.

Wheatley, M. J. (1994). *Leadership and the New Science*. San Francisco: Berrett-Koehler.

Wheatley, M. J. (1999). *Leadership and the New Science* (2nd ed.). San Francisco: Berrett-Koehler.

Wheeler, D. J. (1993). *Understanding Variation: The Key to Managing Chaos*. Knoxville, TN: SPS Press

Wickert, A., & Herschel, R. (2001). Knowledge management issues for smaller businesses. *Journal of Knowledge Management*, *5*(4), 329-337.

Wiig, K. M. (1997). Knowledge management: Where did it come from and where will it go? *Expert Systems with Applications*, *13*(1), 1-14.

Wiig, K. M. (2000a). Knowledge management: An emerging discipline rooted in a long history. In C. Despres & D. Chauvel (Eds.), *Knowledge Horizons* (pp. 3-26). Boston: Butterworth Heinemann.

Wiig, K. M. (2000b). Application of knowledge management in public administration. *Knowledge Research Institute*. Retrieved January 5, 2004 from http://www.krii.com/downloads/km_in_public_admin_rev.pdf

Wijnhoven, F. (2006). Knowledge Management: More than a buzzword. In A. Jetter, J. Kraaijenbrink, H.-H. Schröder, & F. Wijnhoven, (Eds.), *Knowledge Integration* (pp. 1-16). Heidelberg, Germany: Physica-Verlag.

Willumeit, -Ing. H.-P. [2001]. Seven years of EUCARE. *EUCARE*. Retrieved August 25, 2002 from http://www.eucare.de/willue.htm

Wise, J. A., Thomas, J. J., Pennock, K., Lantrip, D., Pottier, M., Schur, A., & Crow, V. (1999). Visualizing the non-visual: Spatial analysis and interaction with information from text documents. In S. K. Card, J. D. Mackinlay, & B. Shneiderman, (Eds.), *Information Visualization* (pp. 442-450). San Francisco: Morgan Kaufman.

Wohl, A. D. (1997). Intelligent text-mining creates business intelligence. *IBM Corporation*. Retrieved November 9, 2002 from http://www-3.ibm.com/software/data/iminer/fortext/download/amipap.html

Wojciech, J. (2000). *Proposal for a GAIN Government Support Team (GST)*. Retrieved August 14, 2002 from http://www.gainweb.org/

Wolford, D., & Kwiecien, S. (2003). Driving knowledge management at Ford Motor Company. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 2, pp. 501-510). New York: Springer.

Worley, S. T. (1999). The new national fire incident reporting system. *Fire Engineering, 152*(4), 111-114.

Yates, J. A. (2000). Business use of information and technology during the Industrial Age. In A. D. Chandler, & J. W. Cortada, (Eds.), *A Nation Transformed by Information* (pp. 107-136). New York: Oxford University Press.

Yin, R. K. (1994). *Case Study Research Design and Methods* (2nd ed.). Thousand Oaks, CA: Sage.

Zack, M. H. (1999). Developing a knowledge strategy. *California Management Review*, *41*(3), 125-145.