# The Influence of Knowledge Management on Managing Organizational Risk

**Emanuel Lauria**
Doctoral Candidate
The Executive Doctorate in Business Program
The Robinson College of Business
Georgia State University
Atlanta, GA 30302-3965

**Dr. Traron Moore**
The Executive Doctorate in Business Program
The Robinson College of Business
Georgia State University
Atlanta, GA 30302-3965

**Dr. Connie O'Brien**
Associate Professor of Accounting
The College of Business
Kutztown University of Pennsylvania
Kutztown, PA 19530

**Dr. Rebecca Staunton**
The Executive Doctorate in Business Program
The Robinson College of Business
Georgia State University
Atlanta, GA 30302-3965

**Subhashish Samaddar, PhD**
Professor of Operations Management and Business Analysis
The Robinson College of Business
Georgia State University
Atlanta, GA 30302-3965

## Abstract

*The purpose of this study is to contribute to the understanding of knowledge management and its relationship to the management of risks that organizations encounter. In this research, we have selected cyber risk in the utility industry as a surrogate for organizational risk. Using publicly disclosed secondary data that includes information on cyber risk, we explored for evidence of what role, if any, investment in knowledge management (KM) plays in the management of risk. Methodologically, we employed a textual analysis of the Item 1A section of annual 10-K reports. We found manifestations in the disclosure data of risk management (RM) and KM, and also investment in KM activities. Further, we show that KM and RM coalesce in the firm as a unified risk – response – resolution sequence, in which investment in KM influences RM mitigation. Our research supports the assertion that "RM is KM", and offers a response to the issue of how KM can contribute to enterprise risk management.*

**Keywords:** Knowledge management, risk management, risk factors, cyber, electric utility holding company, sequence

## *1. Introduction*

Knowledge management (KM) encompasses a defined group of activities that operate across organizational boundaries, and are deployed throughout many different industry sectors (Rodriguez & Edwards, 2009).

Among the goals of KM are to improve the visibility of knowledge, to create a knowledge-based culture and to build a structural framework for knowledge (Davenport & Prusak, 1998). There is a high degree of variation in the level of adoption, depth of sophistication and commitment of financial resources to KM from company to company. The impact of KM is evident in the routines and processes of companies, including those that determine how risk is managed (Neef, 2005).

Risk management (RM) is also a collection of institutional activities. The focus of RM is to ascertain and address the risk of loss companies face from a multiplicity of sources. Its affects span from tactical actions to strategic planning (Rodriguez & Edwards, 2009). While data and information of various kinds and quality flow into RM processes from across the breadth of organizations, knowledge is required to make sense of its meaning (Marshal & Prusak, 1996). Knowledge has been recognized as making a contribution to minimizing risk (Dickenson, 2001).

The relationship between RM and KM is complex. Some industry observers maintain that without KM, RM cannot be successful and in fact, "RM is KM" (Neef, 2005). Nonetheless, there is a lack of clarity in determining the ways in which the loci of KM and RM overlap (Rodriguez & Edwards, 2009). It is difficult for stakeholders to fully evaluate how KM influences RM, or how investment in KM may lead to increased RM effectiveness. The purpose of our research is to contribute to the understanding of KM and its relationship to the management of risks that organizations encounter. This is the first study to explore risk disclosure statements for evidence of RM and KM and in so doing, to attempt to establish how investment in KM effectuates the practice of RM in companies.

We present the results of a study of a pervasive risk in the publicly owned electric utility holding company (EUHC) sector. EUHCs are subject to a wide variety of risks and a substantial degree of uncertainty in the power production marketplace. Awareness of known and arising risks to EUHCs perpetuates the need for a well-defined risk management process (Ericsson, 2009; Linares, 2002; Longstaff, et al., 2000; Mann et al., 1991). Demand growth, price elasticity of electricity, energy and financial market dynamics, commodity costs, environmental regulation and public opinion are representative of the types of exposures facing the industry. It is essential The Influence of Knowledge Management on Managing Organizational Risk that EUHCs have in place effective means to store, move and protect the massive amounts of data and information that are produced in the course of their operations. They must also manage and safeguard the operational IT systems that control power generation and transmission functions. Meeting these objectives is becoming increasingly difficult in light of utility system complexity. Significant challenges arise from the interconnectedness and interdependencies between the numerous separate infrastructures that create the U.S. electricity-producing grid (Longstaff et al., 2000). One fundamental risk encountered by all EUHCs is that which emanates from the digital, or "cyber" domain. Cyber is a prefix that means "computer" or "computer network," as in cyberspace, the electronic medium in which online data transmission and communication takes place (American Heritage Dictionary). Management of these knowledge related activities "must be an essential and natural part of daily operations of various tasks in a EUHC" (Ericsson, 2009).

## *2. Literature Review*

### 2.1. Knowledge Management

The earliest recorded use of a "knowledge-focused management practice" in an institutional setting was at Chaparral Steel Company in 1975 (Wiig, 1997). The practice was integrated into the company's corporate strategy and contributed to the design of its organizational structure. During the 1980s, interest grew in understanding more about how knowledge influences business (Sveiby, 2001). Research expanded to incorporate the emergence of studies on artificial intelligence that were directed toward enhancing learning (Sveiby, 2001). The publication of Hiroyuki Itami's book *Mobilizing Invisible Assets* in 1987 further underscored the value of intangible resources to the conduct of business. Itami observed that U.S. businesses "…do not pay enough attention to protecting and developing invisible assets such as the goodwill of clients, reputation, loyalty and trust in business relationships, because they are not emphasized on the balance sheet" (Sveiby, 2001).

One of the major contributors to the development of modern KM is Robert M. Grant who posited, "the primary role of firms is in the application of existing knowledge to the production of goods and services" (Grant, 1996). This argument paved the way toward a new conception of how knowledge plays a direct and influential role in the ways in which companies operate.

By the late 1990s, KM had evolved into a distinct field of study. The traditional, resource-based perspective of the firm (Grant, 1996) began directly competing with a new, knowledge-based point of view. The recognition by researchers of a rapid transition in the U.S. to a service-based economy coincided with the shift in outlook. Concomitantly, the advent of the Internet accelerated the globalization of business, and with it brought about increasingly open access to many of the elements of the resource-based firm. Many of these elements became imitable, potentially resulting in the diminution or even destruction of competitive advantage. However, proprietary organizational knowledge and the progression toward its systematic management instead became a means to preserving competitive advantage.

Having established that knowledge is critical to business pursuits, and that KM facilitates effective action and increases the potential of the company (Nonaka, 1994), questions arose as to whether knowledge is a process or an object. Alavi and Leidner (2001) responded to this taxonomical issue with the introduction of tacit knowledge. Nonaka (1994) articulated tacit knowledge as a "continual way of knowing." This "way of knowing" is highly personal and draws on the individual's view of life, learning and people. Nonaka and Alavi, and Leidner regard tacit knowledge as being divisible into cognitive and technical components. This would allow, based on applicable circumstances, for knowledge to take the form of both process and object. Alternatively, explicit knowledge is that which can be tangibly managed, recorded and enables recall through access (Nonaka, 1994).

Barclay and Murray (1997) offer a further refinement of KM. The authors describe KM as the process of "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." Alavi and Leidner (2001) describe KM as a collection of four core organizational activities. The first, *knowledge creation* is concerned with developing new content or replacing existing content within the organization's tacit and explicit knowledge bases. Second, *knowledge storage and retrieval*, which is also referred to as organizational memory, is involved with the storage, maintenance and ability to access tacit and explicit knowledge. Third, *knowledge transfer* is the movement of knowledge within, between and across various individuals, groups in the organization. Lastly, *knowledge application* is the purposeful utilization of knowledge to derive additional value in work activities or in the performance of the firm. While there are variations in the literature in the detailed characterization of these activities, the conceptual base is consistent. They will form a framework for our analysis, by which we will examine the companies in our sample group.

**2.2. Risk Management**

Longstaff et al., (2000) propose that *risk* is a quantitative measure of the probability and severity of adverse effects. Precise measures, however, are difficult to achieve due to the degree of uncertainty inherent in the process of assessing risk. Further, the emphasis of risk assessment should not be on obtaining "correct" solutions, but rather on designing strategies that may respond to possible changes and mitigating risk in an efficient way (Linares, 2002). Firms face risk-based decisions and undertake various steps to reduce, eliminate, transfer and accept such risk (Longstaff et al., 2000). This quantification, assessment and mitigation activities form the essence of *risk management* (RM).

Mann et al., (1991) found that effective management strategies for minimizing corporate risk do not impede individual progress or discourage team members. The authors developed a model for the promotion of an effective learning environment, one that facilitates the sharing and creation of knowledge. Various types of institutional knowledge such as access to experts and past research, insights into work-in-progress and peer group problem solving may be directed toward the management of risks.

In general, all organizations face risks and must manage them to survive and compete in the marketplace. The firms that develop and deploy a systematic approach to manage these risks are more likely to gain sustainable competitive advantage over those who do not. Additionally, the rate of structural change impacting industries is significant and likely to continue. There are emerging risks associated with this accelerating pace of change, and these trends will challenge competitors over the short– and long-term horizon. As a consequence, the demand for and supply of a constant flow of information will be critical to manage these dynamics (Mann et al., 1991).

The objective of this research is to study what organizations are doing in managing their risks, and specifically, what role investment in KM may play in this capacity. While there are common elements of RM models found in theory and practice, we sought a recognized, unifying framework to collect and organize data.

One potential avenue is through the standards, security and engineering considerations that are critical to a successful RM effort, particularly in the utility industry. Ericsson (2009) proposed an IT-derived framework which when implemented during times of change provides a basis for risk assessment and mitigation. Ye et al., (2005) present a conceptual structure to facilitate the understanding and assessment cyber attack characteristics, drawn from systems engineering, fault modeling and risk assessment. The focus upon standards, security and engineering are important elements of a successful RM effort, but such a scope is narrow for our purposes. We wish to capture RM in a sufficiently broad context that will align with the ubiquitous nature of cyber risk in most companies, and especially in the utility industry.

Our exploration for an appropriate RM framework also led us to consider adopting a more strategic view of corporate risk management that of enterprise risk management (ERM). The Casualty Actuarial Society Committee on Enterprise Risk Management (2003, p. 8) states, "ERM is the discipline by which an organization in an industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders." The ERM approach to risk is to manage across the full span of the firm, rather than in discrete structural or functional silos. By embedding ERM principles, a deliberate shift in strategy is made from the compartmentalization of risk to the coordination of risk (Nocco & Stulz, 2006).

There are a variety of definitions and methodologies of ERM promulgated in industry. The most widely known exposition of ERM is provided by the 2004 Committee of Sponsoring Organizations of the Treadway Commission, or COSO (Arena et al., 2010):

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The COSO methodology is further developed in Enterprise Risk Management – Integrated Framework. This guidance document presents a three-dimensional integrated model that combines a defined set of corporate objectives, multitier compliance considerations and operational components. Of particular interest are the eight interrelated operational aspects, which provide the basis for our research. This dimension of the COSO model is arranged in a structured pattern. The model begins with 1) a review of the internal environment of the firm, 2) recognition of its objectives and 3) event identification. The protocol then progresses to 4) the assessment of risks from which to develop management decision options. The final four steps are measures of risk mitigation that are characterized as 5) risk response, 6) control activities, 7) information and communication, and 8) monitoring (COSO, 2004). We created a RM analytical framework using a three-part identification, assessment, and mitigation design, which we have employed to organize our data in the next section. The eight operational COSO components are combined into three master activities, which are identification (internal environment, objective setting and event identification); assessment; and mitigation (risk response, control activities, information and communication and monitoring). This consolidation aligns with the core functions of risk management, and captures the systematic detail underlying ERM.

## *3. Context of the Study*

### 3.1. Data Collection

This study involved a group of 55 shareholder-owned electric utility holding companies (EUHCs), whose financial performance is tracked on a quarterly basis by the Edison Electric Institute (EEI) association. The shares of these EUHCs are listed and traded on U.S. stock exchanges. We utilized the 4Q2011 EEI Financial Update report for our analysis. The demographics of this group of companies are diverse with respect to geographic location, number of customers and revenue size. Approximately 95% of the end-user customers in the shareholder-owned segment of the industry are served by these EEI member companies. The value of such a group to our research is that it affords us consistent data points to produce a meaningful representation of the overall electric utility industry.

To conduct our research, we needed to access documentation of organizational profiles that provide meaningful insight into the risk issues of the sample group. We selected each company's annual 10-K report for that purpose. Our decision was guided by the 2005 SEC promulgation, Item 503(c) of Regulation S-K, which created a new disclosure burden in the annual filing process. This additional section of the 10-K, Item 1A.

Risk Factors, is a "discussion of the most significant factors that make the offering speculative or risky" (Federal Register, 2005). The legal intent of Item 1A is for the company to respond with a plain English explanation of all major risks for the benefit of potential investors. The incremental value to investors of divulging what could be characterized as simply a 'laundry list' of potentially substantial exposures to loss has been debated. However, there is research indicating that the risk factor disclosures are a material and important representation of the risks of the firm (Campbell et al., 2011), which lends credibility to our data source as a reliable and consistent discussion of corporate risks.

## *4. Methodology*

### 4.1. Data Analysis

Our approach to the research questions was through a review of the RM and KM literature, presented earlier in the paper, from which we created a framework for analysis. Using that framework, we collected and interpreted data from the 10-K reports. Content analysis is a recognized technique for investigating voluntary disclosures in annual reports (Abeysekera, 2006; Campbell et al., 2011). *[Interviews of subjects from our group of 55 EUHCs to gain insight into operational practices proved difficult to arrange due to compliance and confidentiality restrictions.]* Each of the 10-K reports was assigned a random identification number from 1 – 55 and loaded into edition 10 of NVIVO[1]. The complete risk factor section of each report was extracted as a new source for our analysis. We then conducted a word frequency search to identify the various types of risks disclosed. This initial coding exercise revealed multiple risk categorizations, including regulatory, legislative, litigation, construction, operational, financial and market. These categories were not universal, and frequently contain multiple risk factors. In certain cases, the disclosures are idiosyncratic to the particular organization, while in other cases they are generalizable to the electric utility industry. Given the extensive range of risk data, we elected to narrow scope and selected the cyber risk factor as a surrogate of organizational risk. Our decision was motivated by the ubiquity of cyber exposures in the EUHC sector, and its congruence with KM and RM as having an enterprise-wide imprint. Cyber risk was disclosed by 46 of the 55 companies in our sample, or 84%, with 146 individual references in the Item 1A sections. The data were analyzed in an iterative process, with each of our authors working independently. Subsequent reviews, discussion and updating were repeated across time intervals to maximize inter-rater reliability.

Since the SEC has compelled public corporations to discuss risk factors of significance, we were interested in the ways in which aspects of materiality are expressed in the filings. What is the potential severity of the risks? How widespread is the projected impact? Who are the parties that may experience its effects? The treatment of these questions has implications for the potential application of RM and KM, and informed our examination of the data. However, the SEC has not provided filing corporations with explicit directions to follow in terms of the particular content to include in the risk factors section. As these disclosures do not obligate management to discuss comprehensive resolution strategies to the risks of their organization, we could not be certain at the outset of our research if or how the use of either RM or KM would be stated in the data. A basic review of a sample of the reports indicated that such evidence might indeed not be clearly presented. Consequently, our initial research direction was to look for indications in the data that reasonably infer the utilization of RM activities in the management of cyber risk. We then fit these data into the framework developed from our literature review.

#### 4.1.1 RM Activities in the Subject Organizations

What is actually at risk in EUHCs from a cyber standpoint, and how is this expressed in the disclosure language?

There are certain words and phrases in the risk factors sections that are indicative of risk identification activities being conducted by the filing EUHC. This activity is exhibited by the citation of particular assets that are exposed to cyber risks (Table 1). These identified cyber exposures, or "manifestations", bifurcate into subcategories. Tangible cyber assets have a physical disposition, aligned to the traditional accounting definition of plant, property and equipment. Intangible assets are the various forms of knowledge content that are contained within the tangible asset category.

[1] NVIVO is a qualitative data analysis (QDA) computer software program. Its capabilities enabled our researchers to organize, examine and classify the large volume of non-numerical data from the 10-K reports into a single platform to facilitate this analysis.

Although different in substance, these identified asset classes are intrinsically related and both are exposed to risk. They establish a basis for the balance of our RM framework, and will later translate into the KM analysis.

**Table 1: Risk Identification Activities**

| Subcategory | Manifestations | Inter-rater agreement[4] |
|---|---|---|
| **Tangible asset** | "IT systems", "network", "infrastructure", "grid", "data center facilities", "components", "equipment", "operations", "data processing centers", "data processing systems", "computer hardware", "computer software" | 4/4 |
| **Intangible asset** | "data", "information", "intellectual property" | 4/4 |

[1] The inter-rater agreement represents the final group outcome of the coding process. After the initial independent review of the 10-K data, the four researchers compared coding entries. Differences of opinion were debated and resolved, or a second independent data review of the remaining conflicts was conducted. This additional review was followed by another group discussion, the result of which is displayed in our tables. The ratio should be read as "X researchers out of 4 have agreed".

The SEC guides the expression of the gravity of the identified cyber risk exposures to the extent of how "significant" the risks are. Judgment is required on the part of the filing corporation to make such a determination, and to articulate an appropriate rendering of this significance. The EUHCs in our sample made no discernable attempts to quantify the potential severity of the cyber risks they face, given that this type of estimate is not required under disclosure law. In order to introduce a dimension of materiality to our risk analysis, we used "tone" as a proxy. The tone of disclosure language recognizes the possible manipulation of impressions on the part of the reader that may be made by management. Language manipulation is the subject of research into questions of bias, influence and concealment in disclosure documents (Cho et al., 2010; Campbell et al., 2011). We have recorded in Table 2 entries from the 10-Ks with tonal characteristics that connote higher degrees of risk attached to the asset. This approach to disclosure tone enables us to more richly describe the identified manifestations of cyber risk.

**Table 2: Risk Identification: Significance**

| Subcategory | Tone | Inter-rater agreement |
|---|---|---|
| **Tangible asset** | "sophisticated" | 3/4 |
| **Intangible asset** | "sensitive", "confidential", "proprietary", "personally identifiable", "critical" | 4/4 |

An additional signal of cyber risk severity is expressed by its impact on stakeholders. The impact may come as a result of ownership of, control over, responsibility for or material interest in the tangible and intangible assets. Our research indicates that there are differences in stakeholder impact between the asset subcategories (Table 3). Tangible asset stakeholders consistently manifest as the EUHC itself, communicated as "we" and "our". Given the capital structure of the companies in our sample group, "we" and "our" would also include shareholders. The researchers could not determine the intent of the filing companies in this regard, as these terms were not defined in the risk factors sections.

**Table 3: Risk Identification Activities: Scope of Impact**

| Subcategory | Stakeholder | Inter-rater agreement |
|---|---|---|
| **Tangible asset** | "we", "our" | 4/4 |
| **Intangible asset** | "we", "our", "customer", "employee-related", "shareholders", "suppliers", "business partners", "vendors" | 4/4 |

In contrast, there are multiple stakeholders represented by the intangible asset class, both internal and external to the firm. The wider scope emanates from the mutual claims on the content streams that are housed in and flow across the tangible asset base. Establishing the relative exposure to cyber risk among these various stakeholders is also not addressed in the disclosures.

Having identified categories of EUHC assets subject to risks we turned our attention to risk assessment. In this instance we explored the nature of the risk confronting the identified assets. Our analysis follows the same manifestation-tone-stakeholder model as with the risk identification process (Table 4). Once again, the data diverges into interrelated categories. Risk assessment manifestations reveal an ordered relationship. First, a cyber asset can be acted upon by various events that are outside of normal operating procedures and demand a response to restore functional equilibrium. Next, these events lead to certain outcomes, which are expressed as loss or damage to the firm. Tone words play a role in explicating the

**Table 4: Risk Assessment Activities**

| Subcategory | Manifestations (M) | Tone (T) | Stakeholder (S) | Inter-rater agreement (M\|\|T\|\|S) |
|---|---|---|---|---|
| **Event** | "cyber attacks", "terrorism", "disability", "failures", "unauthorized access", "hacking", "viruses", "acts of war", "other causes", "breach", "malfunctions", "unauthorized control", "human error", "intrusions", "incidents", "misappropriation", "corruption", "leakage", "compromises", "interruption", "deficiencies", "delays", "theft", "disruption", "malware", "damage" | "vulnerable", "hostile", "malicious", "intentional", "deliberate", "man-made", "catastrophic" | "we", "our" | 4/4 \|\| 4/4 \|\| 4/4 |
| **Outcome** | "unable to fulfill business functions", "unauthorized disclosure", "loss of data", "reputation [risk]" | | | |

Assessment manifestations through the use of graphic language. The events can then be characterized by degree of severity ("catastrophic"), motive ("hostile", "malicious", "intentional", "deliberate"), root cause ("man-made") or state of readiness ("vulnerable"). Stakeholder interests in the assessment process are uniformly attributed to the EUHCs.

The final activity in our RM framework is risk mitigation, which are steps undertaken to reduce or eliminate risk (Table 5). Engaging in these activities presents management with decisions that involve complex cost/benefit analyses and capital allocation trade-offs. There is a timing dimension to mitigation that is linked to the occurrence of the assessed event. Proactive risk mitigation efforts are pursued pre-event. They are intended to minimize potential risks and reduce possible losses emanating from those risks. Conversely, a reactive or post-event response will be required to minimize actual losses sustained and to restore full operational capabilities. Tone words associated with the mitigation manifestations are rational statements of possible inefficacy on one hand, and legal disclaimers on the other. They indicate that despite the best intentions of management, mitigation activities may not succeed. These statements are purposely designed to minimize disclosure-related legal risks. Given the responsibility on the part the firm to assure the integrity of business functions, the stakeholders from a mitigation point of view are consistently found to be the EUHCs.

**Table 5: Risk Mitigation Activities**

| Subcategory | Manifestations (M) | Tone (T) | Stakeholder (S) | Inter-rater agreement (M\|\|T\|\|S) |
|---|---|---|---|---|
| **Proactive** | "business continuity planning", "intrusion detection and prevention", "protection", "firewalls", "anti-virus software", "safeguards", "procedures", "IT controls", "compliance", "control environment" | "cannot guarantee", "may not be effective", "despite security measures", "no assurance", "potentially vulnerable" | "we", "our" | 3/4 \|\| 4/4 \|\| 4/4 |
| **Reactive** | "repair [or]replace damaged assets", "disaster recovery", "crisis management" | | | |

In summary, we found evidence of risk identification, assessment and mitigation activities in the disclosure data, which indicates that RM is being actively practiced in our sample group of companies. In the next section, we discuss our exploration for KM activities.

### 4.1.2. KM Activities in the Subject Organizations

We began our research into cyber risk disclosures using a framework that facilitates the classification of RM activities. The next step in the analysis is to examine the data for evidence of KM deployment. Once again, we identify and extract specific manifestations from the disclosure data. The differences in scope between RM and KM as observed in the literature are accommodated in our classification scheme. For KM purposes, tone and stakeholder are less relevant. Instead, we focus on the facilitation of effective organizational action (Nonaka, 1994) through the use of KM. We classify such effective action as "value". A value choice of "static" or "dynamic" enables us to characterize the relative contributions made by KM to the preservation or conversion of the firm, respectively. In this way, we may assess how KM either maintains the present state – static, or contributes to change – dynamic, within the organization.

In the data, we identified manifestations that confront the firm with exigencies in the cyber environment. The EUHC industry risk profile is rapidly evolving. The impact of regulatory pressure alone upon compliance standards, pricing, records retention and the operation of the electric utility grid is rendering existing knowledge inadequate to respond to these challenges. The business must expand its knowledge base beyond that which is currently available to management. Knowledge creation introduces dynamic value, resulting in changes to the asset base of the firm to accommodate shifting conditions.

**Table 6**

In contrast, storage and retrieval manifests as a KM activity concerned with safeguarding and ensuring access to knowledge (Table 7). The value component in this case is static, since the desired state is maintenance of the status quo. While preservation-related manifestations such as "hold", "store", "maintain" and "retain" appear more frequently than retrieval references as in "availability", we treat these two components as a single activity, which is common in the literature.

The EUHCs do not disclose comparative measures of worth for the different types of knowledge stored and retrieved, rendering an assumed equivalence among "data", "intellectual property" and "information" (Alavi & Leidner, 2001).

**Table 7: Knowledge Storage and Retrieval Activities**

| Manifestation | Value | Inter-rater agreement |
|---|---|---|
| "hold large amounts of data", "collect and maintain sensitive customer data", "preserve the confidentiality, integrity and availability of data", "store sensitive data, intellectual property and proprietary information", "secure maintenance of information", "collects, processes and retains information", "secure and reliable storage" | static | 4/4 |

Knowledge transfer in EUHCs is a unifying activity. Knowledge flows across the totality of the EUHC system, a networked environment that links internal and external components. Transfer encompasses tangible assets that move existing and created intangible assets to and from various points of storage for future retrieval (Table 8). This portability is characteristic of dynamic value. Changes in state occur as knowledge is mobilized and made available to multiple consumers for their specific purposes, and re-communicated across the network or externally to other cyber destinations.

**Table 8: Knowledge Transfer Activities**

| Manifestation | Value | Inter-rater agreement |
|---|---|---|
| "continued operation", "interconnected IT systems", "communications among various components", "interconnected nature", "not completely isolated from external networks", "process and monitor", "communication of electronic data", "accessibility through connection the internet" | dynamic | 3/4 |

Knowledge application may be considered from two perspectives in the context of this research. First, the purposeful utilization of existing knowledge to build capabilities and improve performance is, in and of itself, recognized as a KM activity with an established purpose for organizational deployment (Grant, 1996). An additional interpretation of knowledge application is through the rendering of knowledge creation, storage and retrieval and transfer activities themselves. We will address this special functionality in the Findings section as a bridge to RM effectiveness.

In summary, we found evidence of KM activities implicated in publicly disclosed risk factor data: knowledge creation in response to a shifting risk profile, knowledge storage and retrieval for the diverse and massive data inventory housed by firms and the transfer of knowledge across complex networks. Our research objective beyond demonstrating the existence of RM and KM is to establish how KM effectuates RM. In the next section, we show findings of investment in KM activities with the ultimate goal of connecting investment, KM and RM.

### 4.2. Investment in KM

We have constructed frameworks that enable us to recognize and deduce the existence of RM and KM activities. The manifestations are an interpretation of what is occurring in EUHCs, and help us to establish the influence of KM on managing organizational risk. We are also interested in determining whether investment, and in particular as it applies to KM, plays a role in this relationship. The actuation by means of investment is an important signal of institutional commitment to KM. To enable our exploration into the substance of investment activity, we identified through a word search financially oriented manifestations in the data.

Our search parameters included explicit references to investments, costs, outlays, expenditures and capital, as well as activities that implicate the existence of financial investment. The manifestations displayed in Table 9 are made by five EUHCs from the full population of 55 companies upon evaluation of the cyber risks of each respective organization. In accordance with the materiality threshold of the 10-K risk factors section, the quantum of investment, while not specified, is expressed as "significant". The disclosure of these particular activities underscores their importance, given that they represent the outcomes of investment decisions made by management to allocate capital. Our research shows for the first time investment directly associated with KM activities in public risk disclosure data. With this demonstration, we now bring together the full results of our research into the influence of investment in

**Table 9: Investment in KM Activities**

| Investment manifestation | KM activity | EUHC # | Inter-rater agreement |
|---|---|---|---|
| "implementation of new information systems" | Creation and transfer | 11 | 3/4 |
| "increased capital and operating costs to protect information technology" | Storage and retrieval | 27 | 4/4 |
| "expend significant capital to protect against security breaches" | Storage and retrieval | 55 | 4/4 |
| "increased cost of security" | Storage and retrieval | 10 | 4/4 |
| "maintenance, modification and updating, which can be costly" | Creation and storage and retrieval | 23 | 4/4 |

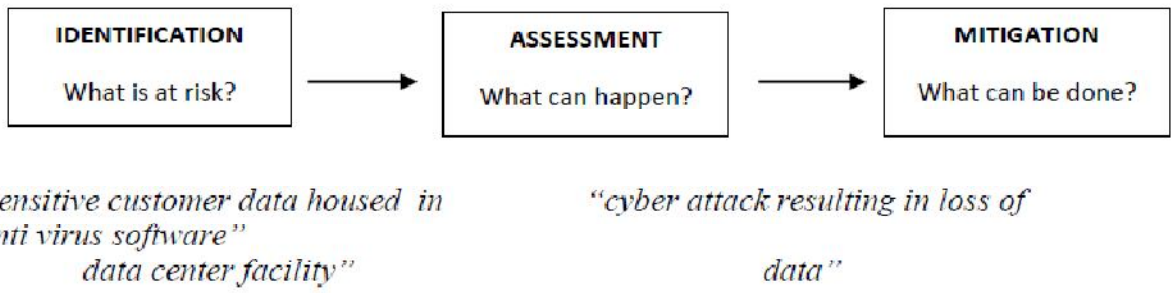
KM on RM.

## *5. Discussion and Findings*

Our findings enable us to establish the co-existence of RM and investment in KM to deal with organizational risk factors. What is not yet clear is the nature of the association between the two. Let us consider, then, how RM and KM coalesce as a composite, multi-activity sequence within the firm.

Abbott (1995) defines a sequence as "an ordered list of elements", or events. The temporal dimension of a sequence may be structured in terms of representative time whereby one event simply follows another. This patterning is not dependent upon measurements of actual clock or calendar time. The individual activities comprising our RM framework occur in a specific sequential process consistent with the operation of other RM models in the literature and in practice to address three key risk-related questions. First, exposures are identified to establish 'what is at risk?' (Tables 1, 2 and 3) Second, a situational assessment is undertaken to project possible outcomes, or 'what can happen?' (Table 4) Lastly, mitigation steps to reduce or eliminate the risks are determined and promote action steps, or 'what can be done?' (Table 5) This linear arrangement of risk identification, assessment and mitigation activities form a simple unitary progression (Van de Ven, 2007), which is presented in Figure 1 using examples from our manifestation data.

**Figure 1: RM activities as a Unitary Progression**

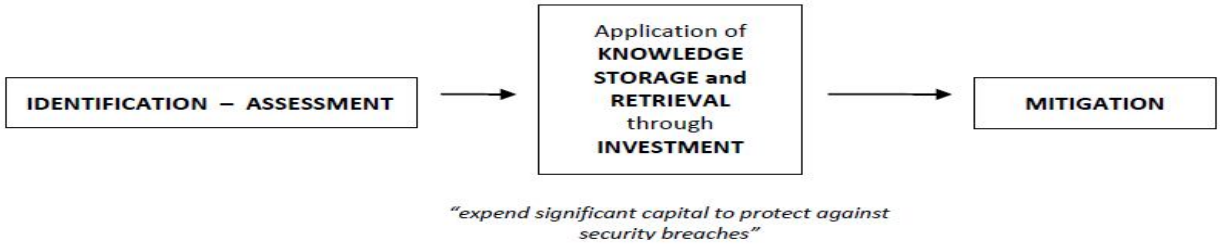


The RM progression from identification to assessment and then to mitigation is targeted at solving risk issues by reducing uncertainty. Answers framed in the appropriate context must be provided for each question in order for the RM sequence to advance. Each activity is considered individually, but in a stepwise pattern. Moreover, there is a logical interplay evident at the initiation of the sequence between identification and assessment to thoroughly delineate the boundaries of risk situations ex ante.

These activities function in tandem to establish the basis on which future action will be taken. Resolution options for these uncertainties are then achieved *ex post facto* through the initiation of risk mitigation activities.

Management will draw upon its resource base to advance the RM progression from the identification-assessment stage to mitigation activities. Among the various types of resources available, knowledge will be demanded to reduce uncertainty and inform decision-making. To facilitate that end, KM activities are designed to identify and map intellectual assets within the firm (Barclay & Murray, 1997). The way in which KM is introduced into the RM process underscores a key difference between the two in organizational practice. Knowledge creation, storage and retrieval, transfer, and application are discretely identifiable activities, but strict linearity among them is not implied (Alavi & Leidner, 2001). The KM activities composing our framework are not specifically ordered as in the case of RM. Additionally, there are not industry-adopted models similar to RM that depend on a standardized progressive sequence. As a result, KM activities can enact individually or in combination with one another. This adaptability provides us with a means to understand the direction of influence of KM on RM. The RM process and KM operate together as a mediated conjunctive progression (Van de Ven, 2007). A KM event, such as investment in knowledge storage and retrieval, will influence the

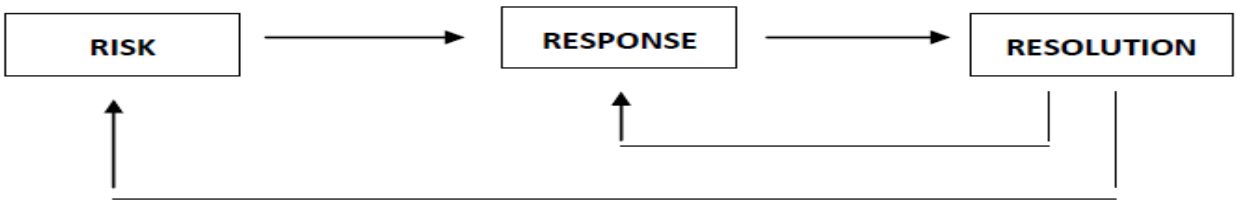
**Figure 2: RM and KM as a Conjunctive Progression**




RM path subsequent to identification-assessment, and prior to a risk mitigation outcome (Figure 2). Our research demonstrates for the first time that this mapping of knowledge that occurs through KM activities to the demand generated by the RM process for the mitigation of risk is evidence of how investment in KM influences RM. The application mechanism exemplifies the purposeful utilization of knowledge to derive additional value in work activities or in the performance of the firm (Alavi & Leidner, 2001). In our progression, significant capital is expended by means of *investment* to protect against security breaches in *storage and retrieval* through the use of anti-virus software *mitigation* from the risk of a cyber attack on customer data in a storage facility rendered through *assessment and identification.*

The synergy between KM and RM represents the formulation of an integrated risk – response – resolution sequence (Figure 3). First, identification and assessment define the nature of the risk and possible loss outcomes. Second, investment in the application of KM contributes to a response to the risk, acting as a mediator in the RM process. Lastly, resolution made post-response in the form of mitigation of the risk is effectuated. This unified RM – KM progression has iterative properties. Final resolution of the risk may require cycling back one or numerous times to engage in additional KM response activities. Similarly, attempts at resolution can raise new identification or assessment issues that will demand responses. When a satisfactory resolution is achieved, the sequence then returns to the identification – assessment stage for consideration of additional risks. Thus, the progression is appropriate for the management of both existing and emerging risks on an individual basis. Beyond this risk-by-risk applicability, the sequence introduces a strategic methodology for envisioning and managing the collective risks of the firm.

**Figure 3: Influence of KM on RM: an Integrated Sequence**




## *6. Conclusion and Future Research Directions*

The use of secondary data from the risk factors section of 10-K reports sourced from the electric utility industry has enabled us to show how investment in knowledge management (KM) effectuates the risk management (RM) process in firms. We found empirical evidence supporting the theoretical expectation that investments in KM activities act as a mediator in a risk – response – resolution sequence, which influences the mitigation of organizational risk. This exploratory study supports Neef's (2005) theoretical assertion that "risk management is knowledge management" by demonstrating the coalescence of RM and KM in an industry setting. Our research confirms the findings of Ye et al., (2005) in their development of a 'system-fault-risk framework' risk mitigation approach. The authors' response to cyber attack risk assessment is achieved via KM of attack characteristics, through which understanding is developed and resolution will be accomplished. Further, we offer an answer from the electric utility industry to the question "how can KM processes contribute to ERM?" proposed by Rodriguez and Edwards (2009). The RM framework we created for our data analysis is explicitly ERM-based. We demonstrate that a contribution is made by KM in the response stage of the integrated RM – KM sequence to influence resolution.

There are several avenues for future research directions to explicate the influence of KM on RM. First, expansion of the secondary data analysis into other risk factors, different industry sectors and manifestations developed from additional sections of the 10-K report will add to our understanding of the risk – response – resolution sequence. Second, our research focus is on qualitative evidence of influence. Variance studies to quantify the measureable impact of investment in KM on actual risk management performance would provide insight to explain how effectively the relationship works in operational settings. Investors may find value in a higher level of transparency around the application of KM processes to mitigate risk, particularly if returns on the expenditures can be quantified in a way that introduces higher levels of certainty into corporate risk profiles. Third, we found evidence that RM and KM integrate within the firm. The execution of this integration, however, is not well understood. How do KM and RM professionals collaborate? What management decision-making occurs that brings KM activities into the RM process, and at what organizational level? Lastly, mediation via multiple KM activities integrating into RM is a more complex sequenced process than that which we present. The incremental value, if any, accruing to RM performance by such means is not known and is an additional research avenue open to exploration.

## *References*

Abbott, A. (1995). Sequence analysis: New methods for old ideas. Annual Review of Sociology, 21, 93 - 113.

Alavi, M. and Leidner, D.E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS Quarterly, 25(1), 107-136.

Abeysekera, I. (2008). Motivations behind human capital disclosure in annual reports. Accounting Forum, 32, 16 - 29.

Arena, M., Arnaboldi, M., and Azzone, G. (2010). The organizational dynamics of enterprise risk management. Accounting, Organizations and Society, 35, 599 - 675.

Barclay, R.O. and Murray, P.C. (1997). What is knowledge management?. Knowledge Praxis,

Available at: http://www.providersedge.com/docs/km_articles/what_is_knowledge_management.pdf

Campbell, J.L., Chen, H., Dhaliwal, D.S., Lu, H. and Steele, L.B. (2011). The information content of mandatory risk factor disclosures in corporate filings. Available at SSRN:

http://ssrn.com/abstract=1694279 or http://dx.doi.org/10.2139/ssrn.1694279

Cihovska, V. and Hvizova, E. (2011). Knowledge management formulates a new system of wealth creation. Economics and Management, 16, 706 - 709.

Cho, C.H., Roberts, R.W. and Patten, D.M. (2010). The language of US corporate environmental disclosure. Accounting, Organizations and Society, 35, 431 - 443.

COSO (1992). Internal Control – Integrated Framework. American Institute of Certified Public Accountants.

Davenport, T.H. and Prusak, L. (1998). Working Knowledge. Boston: Harvard Business School Press.

Dickenson, G. (2001). Enterprise risk management: Its origins and conceptual foundation. The Geneva Papers on Risk and Insurance, 26(3), 360 - 366.

Doyle, J., Ge, W. and McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. Journal of Accounting and Economics, 44, 193 – 223.

Eisenhardt, K.M. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532 - 550.

Ericsson, G. N. (2009). Information security for electric power utilities (EPUs)—CIGRE developments on frameworks, risk assessment, and technology. Power Delivery, IEEE Transactions on, 24(3), 1174 - 1181.

Grant, R.M. (1991). The resource-based theory of competitive advantage. California Management Review, 33(3), 114 - 135.

Grant, R.M. (1996). Toward a knowledge-based theory of the firm. Strategic Management Journal, 17, 109 - 122.

Itami, H. (1991). Mobilizing invisible asset. Boston: Harvard University Press.

Linares, P. (2002). Multiple criteria decision making and risk analysis as risk management tools for power systems planning. Power Systems, IEEE Transactions on, 17(3), 895 -900.

Li, J.J. and Zhou, K.Z. (2010). How foreign firms achieve competitive advantage in the Chinese emerging economy: Managerial ties and market orientation. Journal of Business Research, 63(8), 856 - 862. The Influence of Knowledge Management on Managing Organizational Risk

Longstaff, T. A., Chittister, C., Pethia, R., and Haimes, Y. Y. (2000). Are we forgetting the risks of information technology?. Computer, 33(12), 43 - 51.

Macgillivray, B. H., Sharp, J. V., Strutt, J. E., Hamilton, P. D. and Pollard, S. J. (2007). Benchmarking risk management within the international water utility sector. Part I: Design of a capability maturity methodology. Journal of Risk Research, 10(1), 85 - 104.

Marshall, C. and Prusak, L. (1996). Financial risk and the need for superior knowledge management. California Management Review, 38(3), 77 - 101.

Mann, M. M., Rudman, R. L., Jenckes, T. A. and McNurlin, B. C. (1991). EPRINET: Leveraging knowledge in the electric utility industry. MIS Quarterly, 15(3), 403 - 421.

Neef, D. (2005). Managing corporate risk through better knowledge management. The Learning Organization, 12(2), 112 - 124.

Nocco, B. and Stulz, R. (2006). Enterprise risk management: Theory and practice. The Journal of Applied Corporate Finance, 18(4), 8 - 20.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. Organization Science, 5(1), 14 - 37.

Rodgriguez, E. and Edwards, J.S. (2009). Applying knowledge management to enterprise risk management: Is there any value in using KM for ERM?. Journal of Risk Management in Financial Institutions, 2( 4), 427 - 437.

SEC (2003). Management's report on internal control over financial reporting and certification of disclosure in exchange act periodic report. Available from: http://www.sec.gov/rules/final/33-8238.htm

Sveiby, K. E. (2001). A knowledge-based theory of the firm to guide in strategy formulation. Journal of Intellectual Capital, 2( 4), 344 – 358.

Van de Ven, A. (2007). Engaged scholarship. New York: Oxford University Press.

Wiig, K. M. (1997). Knowledge management: An introduction and perspective. Journal of Knowledge Management, 1(1), 6 - 14.

Ye, N., Newman, C. and Farley, T. (2005). A system-fault-risk framework for cyber attack classification. Information Knowledge Systems Management, 5. 135 - 151.