EDITORIAL PREFACE

Special Issue on Knowledge Management and Risk

Murray E. Jennex, San Diego State University, San Diego, CA, USA

Most Knowledge Management, KM, research focuses on the key issues in KM or on applications of KM (Jennex, 2014). Jennex (2014) identified key issues as including knowledge sharing, knowledge transfer, barriers to knowledge flow, knowledge discovery, knowledge artifacts, KM success, and KM measurement. This special issue of the International Journal of Knowledge Management focuses on one of the least studied issues in KM, security, and more specifically risk in KM. Why this special issue? For balance, KM is about generating value by leveraging what the organization knows to make better decisions, to innovate processes and products, and to improve collaboration and communication in our knowledge workers. All are worthy things to do and worthy of research. But all also have risk and risk management within KM is something also worthy of research yet is something not receiving the attention it deserves.

The National Institute of Standards and Technology (NIST) defines risk as the net negative impact of the exercise of a vulnerability; considering both the probability and the impact of occurrence (Stonebruner, et al., 2007). Alternatively, a risk can also be simply an outcome that in unexpected and can be positive or negative. Note that a risk that is positive can also result in a negative situation if there is too much of a positive outcome, such as more orders than can be filled, more guests than expected, or too much knowledge and/or information (commonly called information overload). Finally, there are three main areas for risk. Technical risk is risk associated with using technologies, be they new, old, or current and can involve technology failure or exploitation of a vulnerability in the technology. Behavioral risk is risk associated with human action and can either be intentional or accidental actions. Legal risk is risk based on not complying with statues and can be intentional or accidental.

My motivation for this special issue is that I spent twenty years as a former United States Navy Nuclear Propulsion Officer and a nuclear engineer in the commercial nuclear industry prior to moving to academia. Nuclear power is a risk focused industry where risk analysis and management drives almost all activities. This has made me a risk focused researcher with respect to crisis management, project management, software development, and knowledge management. Additionally, while researching my dissertation on productivity effects from organizational memory (the precursor to KM) I came across the work of Walsh and Ungson and their discussion on the misuse and abuse of organizational memory that sounded a lot like the risks of organizational memory.

Walsh and Ungson (1991) identified three contexts in which organizational memory could be misused:

- Automatic retrieval of data/information/knowledge may lead to a routine decision response when a non-routine decision response is warranted;
- The controlled retrieval of data/information/knowledge may lead to a non-routine decision response when a routine decision response was appropriate;
- A controlled retrieval of data/information/knowledge may be appropriately activated in an attempt to elicit a non-routine decision response but it may be implemented poorly.

Abuse of the organizational memory occurs when organizational members self-servingly select data/information/knowledge to support positions that serve their political needs rather than the organization's (Walsh and Ungson, 1991). These four generic risks are also applicable to KM and have guided my research into KM risks.

I find that KM and risk has two relationships. The first is the risk of using knowledge and KM. This risk is based on Walsh and Ungson (1991) above and reflects the misuse and abuse of knowledge and the KM system. Examples of this risk include:

1. Failure to identify and capture critical knowledge (Jennex and Zyngier, 2007; Jennex, 2010, 2013, 2014):
   a. Technical risks come from using automated tools to identify and capture critical knowledge with the vulnerabilities typically being in the ontologies and taxonomies used to guide the automated tools;
   b. Behavioral risks occur from personnel classifying critical knowledge intentionally or accidentally not recognizing critical knowledge or failing to capture it when it is recognized;
2. Disclosing critical knowledge to unauthorized recipients (Jennex and Zyngier, 2007):
   a. Technical risks come from exploitation of communication vulnerabilities;
   b. Behavioral risks come from intentionally or accidentally failing to maintain access control lists, posting material to inappropriate forums, not following disclosure processes, and/or falling victim to social engineering attacks;
   c. Legal risks come from intentionally or accidentally not complying with disclosure laws such as those dealing with personally identifiable information;
3. Losing critical knowledge by not capturing it from critical human sources (Jennex, 2014):
   a. Behavioral risk comes from intentionally or accidentally not identifying critical human knowledge repositories and taking actions to capture and store the critical knowledge;
   b. Legal risks come from intentionally or accidentally not complying with required knowledge capture;
4. Losing critical knowledge by not storing it on nonvolatile media (Jennex, 2010, 2013):
   a. Technical risk comes from the failure of storage media, hardware, and/or software;
   b. Behavioral risk comes from intentionally or accidentally not following technology procurement processes, selecting providers without checking their technology, not planning for obsolescence, not testing technologies before applying them or while using them, and/or artificially obsoleting technologies before age requires it;

5. Giving bad advice by not using appropriate knowledge (Jennex, 2012):
    a. Technical risks come from search tools not finding relevant data/information/ knowledge, improperly prioritizing data/information/knowledge, not using integration tools allowing relevant data/information/knowledge to not be incorporated into search results, and/or using visualization technologies that influence decision makers to the wrong option;
    b. Behavioral risk from decision makers intentionally or accidentally focusing on incomplete data/information/knowledge, and/or inappropriately applying data/information/ knowledge;
    c. Legal risk comes from decision makers not utilizing due care or due diligence in assessing data/information/knowledge.

The second relationship between risk and KM is the use of KM to mitigate and/or manage risk. KM can mitigate risk in cases where an organization or individual do not possess knowledge of a domain area that is needed and/or where there is a flood of data/information/knowledge making it difficult for an organization or individual to determine what is important. Examples include:

1. Using KM to overcome security knowledge deficiencies in small enterprises (Dimopoulos, et al., 2004; Jennex, et al., 2004):
    a. Technical risks come from search tools not finding relevant data/information/ knowledge, improperly prioritizing data/information/knowledge, not using integration tools allowing relevant data/information/knowledge to not be incorporated into search results, and/or using visualization technologies that influence decision makers to the wrong option;
    b. Behavioral risk from decision makers intentionally or accidentally focusing on incomplete data/information/knowledge, and/or inappropriately applying data/information/ knowledge. Additional risk comes from KM designers not understanding the domain knowledge needed by the small enterprise;
    c. Legal risk comes from decision makers not utilizing due care or due diligence in assessing data/information/knowledge;
2. Using KM to guide adoption of a new technology for crisis response (Jennex, 2010a):
    a. Technical risk comes from not fully integrating technologies resulting in incomplete data/information/knowledge sets and/or adopting new technologies without fully understanding their limitations and vulnerabilities;
    b. Behavioral risk comes from individuals not understanding the limitations of new technologies, using new technologies without considering security issues, and/or using new technologies in inappropriate ways;
    c. Legal risk comes from decision makers not utilizing due care or due diligence in assessing new technologies before implementing and applying them;
3. Reducing information overload in crises (Murphy and Jennex, 2006, Bressler, et al., 2012):
    a. Technical risk comes from search tools not finding relevant data/information/ knowledge, improperly prioritizing data/information/knowledge, not using integration tools allowing relevant data/information/knowledge to not be incorporated into search results, and/or using visualization technologies that influence decision makers to the wrong option;
    b. Behavioral risk from decision makers intentionally or accidentally focusing on incomplete data/information/knowledge, and/or inappropriately applying data/information/ knowledge. Additional risk comes from KM designers not understanding the domain knowledge needed by the decision makers;

c. Legal risk comes from decision makers not utilizing due care or due diligence in assessing data/information/knowledge, collecting and/or disclosing protected data/information/knowledge, and/or making decisions without considering critical data/information/knowledge.

This special issue pushes the boundary of knowledge associated with KM and risk through four papers previously presented in the Confidentiality, Integrity, and Availability of Knowledge and Data Minitrack of the Knowledge, Innovation, and Entrepreneurial Systems Track at the Hawaii International Conference on System Sciences, HICSS. This minitrack is a community of researchers focusing on security in KM. The track focuses on all aspects of knowledge use including KM.

Three papers focus on risk in KM and one paper uses KM to mitigate risk. The first paper is from Ilona Iloven, Jari J Jussila, and Hannu Kärkkäinen, "Towards A Business-Driven Process Model for Knowledge Security Risk Management" and presents a formalized process for assessing, managing, and mitigating technical, behavioral, and legal risk in KM The second paper is from Christina Sarigianni, Stefan Thalmann, and Markus Manhart, "Knowledge Risks of Social Media in the Financial Industry," and addresses the unique technical, behavioral, and legal risks in KM in financial organizations and provides recommendations for financial organizations to protect critical data/information/knowledge. The third paper is from Marilyn Phelps and Murray E. Jennex, "Ownership of Collaborative Works in the Cloud," and addresses the legal risk to KM when done in a cloud environment and provides recommendations for how to evolve the legal environment around collaborative works created in the cloud. The last paper is from Janine Spears and Tonia San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations" this paper uses knowledge transfer/KM to address the legal risk of disclosing/not protecting critical private data/information/knowledge by non-profit organizations such as hospitals.

I expect that the papers in this special issue will be useful to all studying risk and security in KM and look forward to future submissions on the topics of risk and KM and security in KM.

Murray E. Jennex
Editor-in-Chief
IJKM

REFERENCES

Bressler, G.H., Jennex, M.E., and Frost, E.G. (2012). Exercise 24: Using Social Media for Crisis Response. *The World Financial Review*, March-April, 77-80.

Dimopoulos, V., Furnell, S., Jennex, M.E., & Kritharas, I. (2004, November). Approaches to IT Security in Small and Medium Enterprises. *Proceedings of the 2nd Australian Information Security Management Conference*.

Jennex, M. E. (2010). Preface: Why Knowledge Management? In M. E. Jennex (Ed.), Ubiquitous Developments in Knowledge Management: Integrations and Trends (pp. xviii–xxix). Hershey, PA, USA: IGI Global. doi:10.4018/978-1-60566-954-0

Jennex, M. E. (2010a). Implementing Social Media in Crisis Response Using Knowledge Management. *International Journal of Information Systems for Crisis Response and Management*, *2*(4), 20–32. doi:10.4018/jiscrm.2010100102

Jennex, M. E. (2012). Risk and Reward in Crisis Response. *International Journal of Information Systems for Crisis Response and Management*, *4*(3), i–iii.

Jennex, M.E. (2013). Knowledge Management: The Risk of Forgetting. *iKNOW*, 3(1), 4-7.

Jennex, M. E. (2014). *Knowledge Management: Encyclopedia of Management* (3rd ed., Vol. 7). John Wiley and Sons.

Jennex, M. E. (2014). A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel. *The Journal of Information and Knowledge Management Systems*, *44*(2), 185–209.

Jennex, M. E., Addo, T.B.A., & Walters, A. (2004, May). SMEs and Knowledge Requirements for Operating Hacker and Security Tools. *Proceedings of the Information Resource Management Association Conference IRMA '04*.

Jennex, M.E., & Zyngier, S. (2007). Security as a Contributor to Knowledge Management Success. *Information Systems Frontiers: A Journal of Research and Innovation*, 9(5), 493-504.

Murphy, T., & Jennex, M. E. (2006). Knowledge Management, Emergency Response, and Hurricane Katrina. *International Journal of Intelligent Control and Systems*, *11*(4), 199–208.

Stoneburner, G., Goguen, A., & Feringa, A. (2007). *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems*. Washington, DC: United States National Institute of Standards and Technology.

Walsh, J. P., & Ungson, G. R. (1991). Organizational Memory. *Academy of Management Review*, *16*(1), 57–91.

Murray E. Jennex is a Professor of Management Information Systems at San Diego State University, editor in chief of the International Journal of Knowledge Management*, co-editor in chief of the* International Journal of Information Systems for Crisis Response and Management*, and president of the Foundation for Knowledge Management (LLC). Dr. Jennex specializes in knowledge management, crisis response, system analysis and design, IS security, e-commerce, and organizational effectiveness. Dr. Jennex serves as the Knowledge, Innovation, and Entrepreneurial Systems Track co-chair at the Hawaii International Conference on System Sciences. He is the author of over 150 journal articles, book chapters, and conference proceedings on knowledge management, crisis response, end user computing, international information systems, organizational memory systems, ecommerce, cyber security, and software outsourcing. Dr. Jennex is a former US Navy Nuclear Power Propulsion officer and holds a BA in chemistry and physics from William Jewell College, an MBA and an MS in software engineering from National University, an MS in telecommunications management and a PhD in information systems from the Claremont Graduate University. Dr. Jennex is also a registered professional mechanical engineer in the state of California and a Certified Information Systems Security Professional (CISSP), a Certified Secure Software Lifecycle Professional (CSSLP), and a Project Management Professional (PMP).*