Introduction to Knowledge Management and Information Security Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

Murray E. Jennex
San Diego State University
mjennex@mail.sdsu.edu

During the six years of existence of this minitrack, we have published sixteen papers that focus on the intersection of knowledge management and organizational or individual security. Four themes have emerged:

Theme 1: Protecting Confidentiality of Knowledge. Ilvonen, Jusilla, Kärkkäinen, and Paivarint (2015), Ilvonen, Alnne, Helander, and Vayrunen (2016), and Sarigianni, Thallmann, and Manhart (2016) focus on how to protect shared knowledge either within the organization or outside of organizations where knowledge is shared via social media. Spears and San Nicolas-Rocca (2016) suggest that one way to overcome potential knowledge loss due to security reasons is to build information security capacity skills and offer a case study from the health and human services sector that handle very sensitive client information. Jennex and Durcikova (2014) highlight that KM practitioners and researchers need security skills in order to be able to protect organizational knowledge. Finally, Saha, Paramaswaran, Chakrabarti, and Mahanti (2013) offer a formal analysis of fraud when it comes improper to knowledge sharing.

Theme 2: Protecting Integrity of Knowledge. Additional risk to knowledge loss can originate from the usage of cloud storage and other networking technologies in knowledge management systems. Phelps and Jennex (2015) review the current legal environment surrounding cloud and collaborative KM and make recommendation on how to overcome the gap between legal protection for intellectual property and KM. However, according to Schinagl, Schoon, and Paanto (2016) leveraging IT risk management techniques and the usage of security standards and certification can reduce the risk of knowledge loss. Genre-based assessment of information and knowledge security risk can add additional safeguards to knowledge loss because it identifies organizational communication patterns through which organizational knowledge is shared (Padyab, Päivärinta, and Harnesk (2014)). Jäger and Küng (2017) offer a methodology of how to assess trust of knowledge source and certainty of data through three characteristics (trust of source, certainty of data, and importance of data).

Theme 3: Protecting Knowledge Loss Risk. Knowledge loss not only occurs through improper sharing but also because of departing employees. Jennex and Durcikova (2013) offer a methodology of knowledge loss risk assessment that prioritizes efforts within an organization to capture knowledge from departing employees.

Theme 4: Improving Knowledge of Safe Cyber Behavior. Lot of security research focuses on improving compliance with organizational security policy. Knowledge management techniques including knowledge transfer and training can be of help in this area. San Nicolas, Schooley, and Spears (2014) found that the best outcome to increase compliance with security policy is to provide opportunity to employees to participate in the development of the information security awareness and training programs. In addition, Burns, Roberts, Posey, Bennett, and Courtney (2015) suggest that proper motivation can improve the effect of security education, training, and awareness (SETA) programs. Jensen, Durcikova, and Wright (2017) highlight the need to both publicly acknowledge the contribution to a knowledge management system and provide validation of each contribution. They show through an experiment that doing only one (acknowledgement or validation) does not improve the outcome of correct phishing reports.

This year's papers follow the tradition of bringing papers that are at the intersection of security and KM; both belong to Theme 4. The first paper by Whitney, Jennex, Elkins, and Frost discuss the role Internet in human sex trafficking. This study used knowledge management principles and natural language processing methods to develop an improved ontology of online sex trafficking ads using a new type of indicator, emoticons. The second paper authored by Croasdell, Elste, and Hill examine cyber security awareness training with different awareness methods based on measurements of time, cost, personalization, relevance and interactivity. Results illustrate the potential for the Cyber Clinic model, modeled after the methods used in teaching hospitals to perform

URI: http://hdl.handle.net/10125/50425
ISBN: 978-0-9981331-1-9

triage and treatment in healthcare settings, to be an effective method for educating users about cyber security.

The minitrack co-chairs want to thank authors and reviewers for their work in making this sixth year of the minitrack a success. We encourage authors whose research focus is in the intersection of knowledge management and individual or organizational security to submit their work to this minitrack in the future. Research focusing on cyber security training is also welcome