Introduction to Confidentiality, Integrity, and Availability of Knowledge and Data Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

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

During the five years of existence of this minitrack, we have published fourteen papers that focus on the intersection of knowledge management and organizational or individual security.

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.

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 throght which organizational knowledge is shared (Padyab, Päivärinta, and Harnesk (2014)).

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.

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 are. 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.

This year's papers follow the tradition of bringing papers that are at the intersection of security and KM. Jäger and Küng in their paper titled "Introducing the Factor Importance to Trust of Sources and Certainty of Data in Knowledge Processing Systems - A new Approach for Incorporation and Processing" 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). The second paper authored by Jensen, Durcikova, and Wright titled "Combating Phishing Attacks: A Knowledge Management Approach" explores how an organization can utilize employees to combat phishing attacks through knowledge management practices of knowledge evaluation. Specifically, they 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.

The minitrack co-chairs want to thank authors and reviewers for their work in making this fifth 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.

URI: http://hdl.handle.net/10125/41680
ISBN: 978-0-9981331-0-2
CC-BY-NC-ND