We have heard and read many times in the last several decades that the most important asset of an organization is the knowledge of its employees. To allow an easy access to knowledge, organizations are implementing Knowledge Repositories. While this type of automation made it easy to store and distribute knowledge, it also made it easy to move knowledge outside the boundaries of a company. Organizations put in place many technology-based security measures (firewalls, filtering systems), yet they shouldn’t overlook the human-side of security practices. An organization can have the best security technology in place, yet a careless employee talking or emailing or posting on Facebook about the ‘new development’ at the company bypasses all this security technology with ease.

Furthermore, one can find lot of information about current projects done by a company by searching the web. How can an organization effectively protect its intellectual property remains an answered question. What type of security and intelligence techniques are out that that can protect the IP? What are the best ways to train employees so that they would spot potentially criminal activity among employees? Could crowdsourcing be used in this case, meaning asking employees to vote on a particular issue to determine whether it represents a potential threat? This mini-track seeks papers that investigate issues related to security and protection of intellectual assets and explore how organizations can use security measures to protect their KM practices.

This is the second year for the KM and Security Minitrack at HICSS and it has attracted a total of four papers of which three were accepted for presentation. It is expected that future years will see the minitrack grow as it expands into the KM and security research communities.

The three papers are: Genre-Based Assessment of Information and Knowledge Security Risks by Ali Mohammad Padyab, Tero Päivärinta, and Dan Harnesk. This paper outlines how an information security risk assessment method can be elaborated by knowledge-centric analysis of information assets. The paper uses a genre-based analysis method for identifying organizational communication patterns, through which organizational knowledge is shared. Initial experiences of the method-try-outs by three experienced information security professionals are reported.

Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance by Tonia San Nicolas, Benjamin Schooley, and Janine Spears. This case study investigates end user knowledge of their university’s IS security policy and proposes a new approach to improve end user compliance. The results of this study suggest that users may be contributors to the transfer of IS security policies when provided with an opportunity to participate in the development of an IS security awareness and training program.

Integrating IS Security with Knowledge Management: Are We Doing Enough To Thwart The Persistent Threat? by Murray Jennex and Alexandra Durcikova. This paper posits that KM researchers and practitioners also need to think security and explores how important security skills are to KM practitioners and researchers. A literature review is performed to determine how much attention is paid by KM researchers to security. Additionally, 50 KM job postings are examined to determine if security skills are considered important by those hiring KM practitioners. Finally, a survey is prepared for exploring security attitudes of KM practitioners.

The minitrack co-chairs want to thank authors and reviewers for their work in making this second year of the minitrack a success and we look forward to building this research community in the coming years.