# Introduction to Securing Knowledge, Innovation, and Entrepreneurial Systems and Managing Knowledge Risks Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

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

Ilona Ilvonen
Tampere University
olona.ilvonen@tuni.fi

The purpose of this Minitrack is to focus on research on the intersection of knowledge systems, knowledge management, security, and risk management. It 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.

During th existence of this minitrack, we have published twenty five papers that focus on the intersection of knowledge management and organizational or individual security and knowledge risk. These papers belong to one of the following emerging themes: (1) Protecting Confidentiality of Knowledge.; (2) Protecting Integrity of Knowledge; (3) Protecting Knowledge Loss Risk; and (4) Improving Knowledge of Safe Cyber Behavior.

This year's papers follow the tradition of bringing papers that are at the intersection of security and KM; both span across multiple themes. The first paper by Foli and Durst proposes a holistic model that highlights the interrelationships among factors that contribute to knowledge leakage in collaborative projects. They find that incomplete contracts and insufficient technological competence are the principal factors contributing to knowledge leakage within collaborative projects. They also provide significant methodological contributions in the knowledge risk and leakage literature by their use of ISM and MICMAC techniques. With their model Foli and Durst demonstrate the complexity of knowledge leakage, an issue much discussed also in this track in previous years.

The second paper by Lathrop, Croasdell and Elste explores the ever current dilemma of small and middle businesses (SMB): how to navigate the digital transformation era and nurture cyber security competence and readiness with the limited resources and capabilities available. They propose a model for SMBs to enhance their cyber capabilities with cybersecurity assessments and regular training provided by the National Guard's Defensive Cyber Operations Element (DCO-E). Leveraging the capabilities of the DCO-E, in effect a "national cybersecurity squad," to support a national cyber readiness and education campaign could be an effective method to enhance the cybersecurity of SMBs. This model could be adapted also to other national contexts, and it would be interesting to see comparative studies of similar practices in other countries in the future.

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

URI: https://hdl.handle.net/10125/103229
978-0-9981331-6-4