

Introduction to Securing Knowledge, Innovation, and Entrepreneurial Systems and managing Knowledge Risks Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

Murray E. Jennex
West Texas A&M
mjennex@wtamu.edu

Iлона Ilvonen
Tampere University
Iлона.ilvonen@tuni.fi

This minitrack provides a venue for innovative research that focuses 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 the existence of this minitrack, we have published twenty seven 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 minitrack features one session with three papers. The first paper authored by Johannes Paul Zeiringer, Jürgen Fleiß, and Stefan Thalmann titled, "*Data Anonymization as Instrument to manage Knowledge Risks in Supply Chains.*" This paper explores the challenges of managing knowledge risks in modern, interconnected, and digitalized supply chains. The authors highlight the dilemma faced by supply chain partners in balancing knowledge sharing and protection, as sharing data can lead to unintentional disclosure of competitive knowledge. To address this issue, the paper suggests using data anonymization as a solution. The study involves a vignette study with 1,000 participants, utilizing an existing data anonymization tool to investigate the impact of decision support, in the form of a tradeoff visualization, on knowledge sharing. The results demonstrate that the presence of an anonymization tool, along with decision support, increases knowledge sharing. Despite concerns about risk, participants are willing to share data when the process is made transparent and beneficial. This approach can help facilitate knowledge sharing in supply chain management and foster innovation.

The second paper titled: "*Designing Game Based Microgames as Intervention for Health*

Misinformation," is authored by Lindsay Grace, Victoria Orrego Dunleavy, Regina Ahn, and Danny Mayo. This paper presents insights gained from the design and implementation of three small-scale game interventions aimed at enhancing audience resilience to health misinformation and disinformation. Drawing from concepts such as inoculation theory and transportation theory, and tailoring objectives to the specific intervention context, the researchers developed three distinct games to bolster resistance to misleading health information. The study involved conducting semi-structured interviews with the target audience, healthcare providers, and community educators, resulting in positive feedback regarding the potential of microgames to combat misinformation in health-vulnerable populations. The paper outlines the design process, implementation, and feedback gathered from the intended audience. Notably, the feedback highlighted that narrative-based interactive fiction garnered the highest appeal and potential efficacy, followed by a social media simulation, with a trivia game ranking lowest in terms of appeal and potential effectiveness.

The last paper titled "*Assessing and Mitigating the Risk of Critical Knowledge Loss in Organizations: Insights from COVID-19 and the Great Resignation,*" is authored by Murray Jennex, Alexandra Durcikova, Iлона Ilvonen, and Jeffrey Babb. This study addresses the pressing issue of knowledge loss and employee turnover induced by the COVID-19 pandemic. Preserving critical knowledge is paramount for organizational success, yet the rise of remote work and the "Great Resignation" have disrupted traditional knowledge-sharing practices. The study's objective is to adapt Jennex's (2014) knowledge loss risk model to account for these new challenges. Drawing insights from literature on the "Great Resignation" and prior research on knowledge loss, the study puts forth hypotheses for additional contributing factors. A survey was conducted to investigate these factors, uncovering four key influences on employee departure: the absence of remote work or flexible hours, the provision of remote work equipment and

technical support, the preference for flexible hours based on household size, and the necessity of high-speed internet for remote work. These discoveries will be integrated into the Jennex knowledge loss risk predictor model, offering a more comprehensive framework to address the evolving dynamics of knowledge retention in the post-pandemic era.

The minitrack co-chairs wish to express their sincere appreciation to both authors and reviewers for their indispensable contributions, which have been paramount to the minitrack's success over the years. We invite authors dedicated to exploring the nexus between knowledge management and individual or organizational security to consider submitting their research to our minitrack in upcoming sessions. Additionally, we welcome research centered on cybersecurity training.