Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

# Introduction to Security in Knowledge Systems and Knowledge Management Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

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

Data has been labeled "the new oil" of the next century. Ensuring data confidentiality, integrity, and availability is of utmost importance to all organizations. Employees in the following two types of roles are usually involved in decisions regarding data: knowledge managers and cybersecurity managers. These employees (together or separately) identify data needs, provide access to data, promote usage of data, and create the infrastructure so that data stored safely, transported safely, and is accessible. During the eight years of existence of this minitrack, we have published nineteen papers that focus on the intersection of knowledge management and organizational or individual security. 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 spam across multiple themes. The first paper by Thalmann and Ilvonen discusses the need to investigate knowledge risk incidents. The authors argue that knowledge risk incidents have a negative impact on a business and that knowing the potential attacker and their motivation is important for employing successful preventive knowledge protection measures. Also, some knowledge risk incidents are not preventable and therefore planning for knowledge risk incidents in important so that organizations can recover faster. Thalmann and Ilvonen argue that organizations need to develop reactive measures that should be employed after an incident happened.

The second paper discusses the legal and risk management issues that organizations must address when it comes to data and knowledge derived from data. Paper by Jennex and Durcikova tackles this issue and provides a knowledge management risk assessment framework. This paper builds on the previous generic risk assessment framework and the Knowledge Security Risk Assessment Framework to create a risk assessment for knowledge management. This addition to the framework contributes to the current research and practice, by providing a KM/knowledge system-specific threat analysis and a template that can be followed to not only capture the knowledge asset but also to capture the potential threat, it's likelihood, impact, risk score in an easy to understand fashion that streamlines the whole process. Previous research that discussed risk in KM did not provide such a step-by-step approach that is repeatable in any organization.

The minitrack co-chairs want to thank authors and reviewers for their work in making this eight-year 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/10125/64348
978-0-9981331-3-3