Introduction to Intellectual Property and Security Minitrack

Alexandra Durcikova  
University of Oklahoma  
alex@ou.edu

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

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 third year for the Intellectual Property and Security Minitrack at HICSS. The three papers are: Assessing the Role of Security Education, Training, and Awareness on Insiders’ Security-related Behavior: An Expectancy Theory Approach by AJ Burns, Tom Roberts, Clay Posey, Rebecca Bennett, and Jim Courtney. This paper discusses that despite wide-spread agreement across industry and academia on the importance of security education, training, and awareness (SETA) programs, relatively little scholarship has been devoted to understanding the effectiveness of SETA on motivating security-related behaviors. Employing expectancy theory, we make a multi-dimensional assessment of the motivational influence of SETA on two disparate security-related behaviors (a proactive and an omissive behavior).

Knowledge security risk management in contemporary companies - toward a proactive approach by Ilona Ilvonen, Jari Jussila, Hannu Kärkkäinen, Tero Paivarinta. This paper discusses how traditional information security management models tend to concentrate on the technological viewpoint to secure existing information assets. However, the use of contemporary approaches for knowledge creation and sharing, offer new important possibilities for making use of internal and external knowledge. Simultaneously, their implementation involves changes in technologies, as well as a change of work processes and communications. Hence, knowledge security risk management should be developed from the current focus on relatively static containers and information assets towards a more proactive management of the potential future risks of knowledge sharing. This paper introduces a proactive process for managing knowledge security risks and reports experiences from its use by professionals with experience in various topics of information and knowledge security.

Yours, Mine, or Ours: Discussing Ownership of Collaborative Works in the Cloud by Marilyn Phelps and Murray Jennex. This paper discusses how increased usage of cloud storage and other networking technologies in knowledge management systems leave companies vulnerable to loss of proprietary rights as intellectual property law struggles to keep up with these advances. This paper reviews the current legal environment surrounding cloud and collaborative KM, discusses the implications for KM, and makes recommendations for how gaps between legal protection for intellectual property and KM can be overcome/corrected.

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.