Introduction to Knowledge Management and Information Security Minitrack

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

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

The purpose of this Minitrack is to focus on research on the intersection of knowledge management and organizational or individual security. Specifically, 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. While this knowledge can be a target of sophisticated cyber-attacks or fraud, most likely the leaking of knowledge can happen because of careless organizational practices, asset misuse, or behavior of employees. Organizations put in place many technology-based security measures (firewalls, filtering systems) to guard against attacks, yet it is not that easy to guard against 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 unanswered question. What type of security and intelligence techniques are out that that can protect the intellectual property? What are the best ways to train employees so that they would spot potentially criminal activity, such as fraud, 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? Could implementation of KMS potentially cause legal problems because some KM artifacts could be uncovered during discovery and used as evidence against a company?

This minitrack 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. Possible topics include, but are not limited to:

- Securing intellectual assets
- Filtering messages regarding current business practices on social media (e.g., Facebook, LinkedIn)
- Legal concerns when implementing KMS
- Techniques used to scan employee communication channels (e.g., email, Facebook, text messages)
- Security strategies within and outside the company boundaries
- Training employees on potential threats to security breaches
- Preventative measures to secure KM assets
- Knowledge loss risk management
- Impact of immigration and cultural issues on potential KM security breach
- Using KM security to mitigate impacts of retirement and worker transience
- Measuring risk of knowledge loss due to security breach
- Security models and architectures for knowledge systems
- Modeling risk in knowledge systems
- Tradeoffs in knowledge systems between security and knowledge sharing
- Technologies for knowledge system security