Chapter 15

Knowledge Systems and Risk Management:
Towards a Risk and Threat Assessment Framework

Murray Eugene Jennex

https://orcid.org/0000-0003-4332-1886
San Diego State University, USA

Alexandra Durcikova
University of Oklahoma, USA

ABSTRACT

Knowledge is the most important asset that a company can have. Thus, it is imperative that this asset is safeguarded just like generic information assets. However, knowledge management (KM) and knowledge systems are different than traditional information systems with different threats and different operational requirements. Information security professionals recognize that risk assessment is the cornerstone to information security. The authors build on this perspective and propose that risk assessment techniques need to be applied to KM too to properly safeguard this asset. They discuss risk assessment frameworks and build on a KM/knowledge system specific risk assessment framework with a step-by-step guideline for KM/knowledge system specific threat assessment.

INTRODUCTION

Whitman and Mattord (2019) quote Sun Tzu Wu on the importance of knowing yourself and knowing your enemy as a key to success in battle, or in designing and implementing information systems security. To accomplish the knowing of yourself and your enemy the corner stone of information systems/cyber security is the process of risk assessment. Risk assessment is used to know yourself by identifying data/information/ knowledge/technology assets (henceforth simplified to knowledge assets) and assigning. Risk assessment helps organizations know the enemy by determining the threats that could attack the organization's knowledge assets. Risk management then uses these inputs to analyze the overall risk to the knowledge asset and determine the controls to be used to mitigate or remove the risk. All major security frameworks include a risk assessment and management process. For the United States the Nationals Institute of Standards and Technology (NIST) provides the risk management framework (RMF) as described in special publication, SP 800-12 rev 1 (2012), An Introduction to Information Security, SP 800-37 rev 2 (2018), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, and SP 800-53 rev 5 (2017) (draft), Security and Privacy Controls for Information Systems and Organizations. A similar process is outlined by the International Standards Organization (ISO). ISO27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements and ISO7005:2018, Information technology -- Security techniques -- Information security risk management.

While these are fine risk frameworks, they are generic in nature and are not tailored specifically to knowledge management, KM, or knowledge systems. We do not claim that KM/knowledge systems are so unique as to require their own risk frameworks or that the above-mentioned risk frameworks are not useful. We are stating that KM/ knowledge system managers will do a better job of risk assessment/ management of KM/knowledge systems if they have tailored guidance, specifically in two areas: threat assessment and risk analysis. Why do we think KM/knowledge systems need special guidance? We argue that the purpose of KM and knowledge systems are to support the sharing and application of knowledge by supporting decision making, throughout the organization to achieve organizational goals. Since the purpose is to share knowledge the tenets of information security are inherently at odds with KM/ knowledge systems. It is our opinion that information security is still needed but should be applied in ways that recognize the uniqueness of knowledge sharing and decision processes. Jennex and Durcikova (2014) examined the integration of KM and security and found that security was not integrated into the KM job functions. Thus, the purpose of this paper is to provide specific guidance and requirements for KM/knowledge systems threat assessments and risk analysis. In addition, this

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/knowledge-systems-and-risk-management/244892

Related Content

Bayesian Belief Networks for Data Cleaning
Enrico Fagiuoli, Sara Omerinoand Fabio Stella (2008). *Mathematical Methods for Knowledge Discovery and Data Mining (pp. 204-219).*
www.irma-international.org/chapter/bayesian-belief-networks-data-cleaning/26141

Semantics Enhancing Knowledge Discovery and Ontology Engineering Using Mining Techniques: A Crossover Review
Elena Irina Neaga (2007). *Knowledge Discovery and Data Mining: Challenges and Realities (pp. 163-188).*
www.irma-international.org/chapter/semantics-enhancing-knowledge-discovery-ontology/24906

First Results of Formalization of Drilling Knowledge by the Event Bush Method
Pavel Komar, Alexander Khokhuliaand Yuri Gatchin (2018). *Dynamic Knowledge Representation in Scientific Domains (pp. 354-366).*
www.irma-international.org/chapter/first-results-of-formalization-of-drilling-knowledge-by-the-event-bush-method/200184

A Perspective on Data Mining Integration with Business Intelligence
Ana Azevedoand Manuel Filipe Santos (2011). *Knowledge Discovery Practices and Emerging Applications of Data Mining: Trends and New Domains (pp. 109-129).*
www.irma-international.org/chapter/perspective-data-mining-integration-business/46893

Implementation of Data Mining Algorithm With R
C. Deisyand Mercelin Francis (2019). *Sentiment Analysis and Knowledge Discovery in Contemporary Business (pp. 92-125).*
www.irma-international.org/chapter/implementation-of-data-mining-algorithm-with-r/210966