Improvement and Maturity of the Information Security Risk Management Process

Angela Jackson-Summers
Kennesaw State University, Angela.G.Jackson-Summers@uscga.edu

SUMMARY

With alarming rates of increasing information security threats and growing information security concerns among IT executives, this proposed study is designed to address the maturity and effectiveness of information security risk management (SRM). SRM is an organizational, continuous process that involves integration among other organizational processes. SRM also includes controls serving as countermeasures, policies, safeguards, and procedures that work to address security risks. As facets of SRM, maturity refers to the completeness and capability of continuous improvement, and effectiveness regards the level of usefulness of process methods. To help strengthen existing SRM organizational processes, this study aims to address the following questions: How can organizations strive to mature SRM? How can organizations improve SRM effectiveness?

Given the intrusive nature of SRM, the research methods to be used in past SRM studies have been designed with caution. An interview-based approach using the resource-based view theory and a capability maturity model will be used in this study. Interviews of three (3) to five (5) Chief Information Security Officers (CISO), or persons in senior management like roles, will be conducted. While a small number of study informants have been met with criticism in the past research, research rigor can be applied to a small sample rendering rich results. Using the laddering and critical incident techniques, planned interview questions derived from Spears and Barki (2013) and the ISACA RiskIT Process Model Framework (ISACA, 2009) will be used.

The interview data will be collected, analyzed, and interpreted to address SRM effectiveness. Also, the interview data will be used to address SRM maturity. In addressing SRM maturity, the Software Engineering Institute's (SEI) Capability Maturity Model Integration for Services (CMMI-SVC) framework is adopted, because of its use for integrated process improvement assessments. CMMI-SVC is comprised of twenty-four process areas of which the Risk Management (RSKM) model encompasses three maturity levels to organizational improvement. The three maturity levels are defined as 1 (Initial), 2 (Managed), and 3 (Defined). Textual analysis of the interview data will be performed and applied to the RSKM model. The study's findings will be verified and prepared for reporting.

The study's results will be captured and presented. Planned contributions from this study include building upon the existing body of knowledge in the areas of SRM, and the resource-based view theory. Also, the use of the CMMI-SVC framework will serve as an alternative capability maturity model approach for

academic researchers and practitioners when considering processes that are integrated among other processes.