Combining the Extended Risk Analysis Model and the Attack Response Model to Introduce Risk Analysis

Randall Reid
University of West Florida, rcreid@uwf.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp

Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

https://digitalcommons.kennesaw.edu/ccerp/2016/Academic/9

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.
Abstract
This paper uses the Extended Risk Analysis Model to introduce risk analysis in a classroom setting. The four responses to an attack, avoidance, transference, mitigation, and acceptance are overlaid on the Extended Risk Analysis Model to aid in the visualization of their relationship. It then expands and updates the cyber insurance portion of the Extended Risk Analysis Model.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
Only an abstract and summary are published in the Proceedings. The complete article can be found in the Journal of Cybersecurity Education Research and Practice.
SUMMARY

This paper expands the Extended Risk Analysis Model (ERAM) to include the 4 responses to an attack model (4RAM). The article demonstrates how vulnerabilities from the ERAM model can be overlaid by the response option of applying safeguards, how insurance from the ERAM model fits with transference of risk from the 4RAM model, how controls from ERAM aligns with the 4RAM response of reducing the impact, and ERAM acceptance and the 4RAM option of acceptance align.

A subarea of this presentation is the current state of cyber-insurance which is part of the transference option. Cyber insurance has grown steadily and is currently a $2 billion dollar per year market. One of the major differences between cyber insurance and general liability insurance is that cyber insurance focuses on intangible assets while an organization’s general liability tends to focus on physical assets. Cyber insurance is basically divided into two groups. The first group is referred to as first-party exposure, which covers damage and costs directly incurred by the organization. First-party exposure also includes costs such as the loss or damage to the information systems, the payment of cyber-ransoms and the actual theft of money from the organization. First-party also covers denial of service, business interruption and reputation losses. Third-party insurance, the second group, covers the costs that are paid to other groups or individuals outside of the organization, including impacts on the customers and legal costs.