Aous Al Salek
aous.al.salek@his.se
lnkly.se/CybEk
University of Skövde
Presentation Abstract

Cybersecurity Economic Model

A Path to Adoption

In the evolving digital threat landscape, organizations are under increasing pressure to make informed cybersecurity investment decisions. While numerous cybersecurity economic models have been developed to aid such decisions, their practical adoption remains limited. This research aims to bridge the gap between theoretical models and organizational practice by systematically investigating the characteristics of existing models, the barriers to their adoption, and designing tools to support effective implementation. The study is structured around three core research questions: (1) What are the characteristics, strengths, and limitations of existing cybersecurity economic models? (2) What key challenges hinder their adoption in organizational contexts? (3) How can a practical framework and decision-support tool be developed to assist organizations in selecting and applying appropriate models?

To address these questions, the research adopts a mixed-methods research strategy structured into three sequential phases. Phase 1 involves a systematic literature review (SLR) and qualitative interviews with industry experts to map the landscape of existing models and uncover contextual adoption challenges. Phase 2 transitions to a quantitative survey targeting cybersecurity decision-makers in Swedish organizations, analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). This phase empirically tests hypotheses related to organizational readiness, perceived complexity, and institutional influences. Phase 3 applies Design Science Research (DSR) to construct and evaluate a context-sensitive decision-support model. The model will be validated through iterative workshops and real-world case studies involving diverse organizational types.

Data collection methods are carefully chosen to align with the phased design: the SLR ensures a comprehensive theoretical foundation; interviews provide rich, contextual insights; and the survey allows for empirical validation and generalization. Analytical techniques include thematic analysis for qualitative data and PLS-SEM for quantitative modeling, complemented by a factor analysis to ensure measurement validity.

The anticipated outcomes of this research include a validated taxonomy of cybersecurity economic models, empirically grounded insights into adoption barriers, and a decision-support tool tailored to organizational needs. Beyond academic contribution, the study offers actionable solutions for practitioners aiming to make economically sound cybersecurity investments. The long-term goal is to enhance model adoption rates, improve investment decision-making, and support regulatory compliance. By integrating interdisciplinary theory with applied research methods, this project aspires to advance both the science and practice of cybersecurity economics.