8-10-2022

Optimizing Outcomes in Security Organizations

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Optimizing Outcomes in Security Organizations

TREO Talk Paper

Herb Mattord
Kennesaw State University
hmattord@kennesaw.edu

Kathleen Kotwica
Security Executive Council
k2kotwica@secleader.com

Michael Whitman
Kennesaw State University
mwhitman@kennesaw.edu

Abstract

The optimization of security operations in larger organizations has often centered around discussions of the relative degree of convergence of the physical security functions and the cybersecurity functions. Historically the term cybersecurity as is being used here has been referred to as information security or information protection. The terminology for physical security as used here is often identified as corporate security historically and is emerging to be referenced as 'global security and risk management'.

In a collaborative effort with an academic group and a security advisory group, it was determined to explore the factors to be considered when larger organizations make decisions about the placement, governance and operational strategies are evaluated and proposed for update or revision. A broad multipart project has been conceived to explore this topic. This initial study will quantify some of the precursors that influence optimization outcomes in security function convergence, present these criteria as a survey, and take a snapshot of these criteria in the practice setting. A subsequent study will use individuals who have responded to the survey to identify those from organizations that exhibit characteristics from many difference degrees of convergence and optimization. Those individuals will be interviewed to develop additional understanding of the complexities of security convergence and optimization.

While convergence is generally recognized as inevitable or in-progress for most situations, the actual effects that converged organizations experience should be researched more to better determine what methods are effective. Much discussion revolves around addressing issues that arise because of convergence, and therefore it is logical to assume that these issues will create problems should they not be attended to properly. Our research here is in light of observations that convergence is often recognized as inevitable or in-progress for most situations. Yet, the actual effects that converged organizations experience should be researched more to better determine what collaborations are effective.

Historically we have used the term 'convergence' to talk about this phenomenon of inevitability. This has been in place for decades, but there is a challenge to this. First, it really is more difficult than one imagines defining exactly what it means to converge security. There is not just one way to define what convergence can do and deliver and simply comparing what might result from so called convergence will vary from one organization to the next. More philosophically, the oft referenced 'path to convergence' somehow connotes that there is an optimum state at the end of a series of converging aspects that is somehow expected to be superior to other ways of collaborating. We propose that the phenomenon we are all describing might better be called "the degree of collaborative optimization" and this research effort seeks to find the indicators of effective collaborative optimization.

Among the trends noticed was that three factors seem to drive the Security Collaborative Optimization (SCO) level of any organization at any particular moment in time: Management Will, Culture, and Exigency. The planned stream of research will seek to document ways to measure security optimization and how to make such measurements.