Key Findings from

THE STATE OF SECURITY MANAGEMENT

A Baseline Phenomenological and Empirical Study

Funded by

ASIS FOUNDATION™

MODULE 5:

Manage Parochialism in the Security Management Field

Security executives must recognize and manage potential parochialism—defined as a limited or narrow outlook—within themselves and their organizations. Parochialism may promote discord among security professionals, partners, and vendors and may also reduce the ability to manage risk proactively and effectively. Adopting an enterprise security risk management (ESRM) mindset will help diminish the adverse impact of parochialism.

It is most likely that some degree of parochialism or narrow-mindedness has always existed in the security field. Competition for resources, attention, and influence among various subspecialties or disciplines of security can easily lead to narrow attitudes and constricted behavior.

Parochialism is evident in several aspects of security practice, such as approaching security risk management from a governance or compliance perspective versus having more of an assets protection focus. This is an important, real-world distinction because decision makers may need to choose whether to focus on the risk of noncompliance with a standard or regulation versus the risk of an actual loss event (crime, loss of life, injury, operational disruption, etc.).

Also parochial is the assumption that all organizations are like your organization. Security professionals and policy makers must understand that protective tools, techniques, and strategies that are appropriate and effective in a large corporation may not work in small, medium, and entrepreneurial organizations—and that what works in one part of the world may not work elsewhere. Security silos (cyber, physical, personnel, homeland, and other security disciplines) may also lead practitioners to think and act in an insular fashion.

Today, an obvious tension exists between the cyber security and traditional security arenas. In fact, a new term (operational security) has come into common use to describe traditional security. Unfortunately, "operational

security" has other meanings in other, related sectors, such as law enforcement and the military. This is one of the difficulties brought about by repurposing terms without a thorough, collaborative thought process and research effort.

In 2020, a number of seasoned security professionals expressed the position that "today, everything is digital." This implies that all security disciplines other than cyber are irrelevant, and only digital/electronic assets are worthy of protection. In fact, one individual questioned whether there are still truly any organizational assets other than digital. This idea is counter to founda-tional concepts such as enterprise security risk management (ESRM), the all-hazards approach, and a sound asset protection philosophy.

When asked about changes in the security management field, one survey respondent answered as follows:

> *Lack of clarity among many businesses about the difference between cyber and physical security. Many see them as part of the same discipline, but the skill sets are dramatically different. Sort of like saying police and fire are both first responders and either can handle any situation. Training, skills, and equipment are totally different.*

A few examples demonstrate the overemphasis on cybersecurity:

- *CSO Magazine* focuses almost exclusively on cyber topics even though it exists to present informative discussion on all topics of concern to chief security officers and security executives.
- A number of books have been published in the past five years claiming to address "risk management" but actually covering only cyber risk management.
- The term "information security" is often used synonymously with cybersecurity or information technology security whereas its true definition is far broader and includes a variety of traditional security strategies to protection information in any form, along with cybersecurity. In essence, the term has been hijacked by the cyber community, which causes confusion and consternation.

SECURITY THOUGHT LEADER PERSPECTIVE:

A Broad View of Security

"Cybersecurity has risen to the top overall management concern. But conventional issues, such as business continuity planning, workplace violence, employee selection, privacy concerns, and many others, continue to challenge the high-performing security operations manager."

–Robert McCrie, 2016
Security Operations Management

Aon's *Global Risk Management Survey* (2019) states:

> *Our research has emphasized that risk management needs to continue to evolve…as an enterprise-wide, rather than siloed, approach and function. In par-allel, risk managers of tomorrow should continue to…ensure risk is identified, assessed and managed in an integrated way across the organization.*

In our study, over 44 percent of respondents noted that integrating security disciplines was one of their key challenges as a security executive.

One strategy is to focus on the end state—management of an organization's security-related risks—rather than

individual disciplines that contribute toward that objective. This assists in viewing the contemporary battle between cybersecurity and "other" security through a different lens. Security, and hence, security management, is not a simple or straightforward endeavor. It is a multi-dimensional and increasingly complex profession wherein professionals hone and leverage a variety of diverse and interdependent tools for managing security-related risk, ultimately allowing an organization to accomplish its strategic objectives in the most safe and secure manner possible.

The fifth in a series of nine modules, this paper explores the findings of an ASIS Foundation study conducted by Kevin E. Peterson, CPP, CIPM II and Joe Roberts, Ph.D. in 2020 and 2021. To download the full ***State of Security Management*** report, visit *asisfoundation.org*.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters, and organizations. Online at *www.asisfoundation.org*.