Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION™

FINDING FOUR:

SECURITY PROFESSIONALS NEED TO ENGAGE BETTER WITH CORPORATE DECISION MAKERS

Security, along with other risk disciplines including safety, business continuity management, and crisis management, have drawn on similar thematically structured models, captured as standards to guide and document their specific diagnosis risk tasks. However, such models in their current structures lack explicit directions to identify, engage, and communicate directly with key decision makers. Instead, focusing on broad process as opposed to recognizing the significance of the decision maker in the organizational structure and management strata.

The study found that security risk models and their usage require adjustments to meet the structural and stratum of corporate organizational risk. Focus group participants saw current security risk models as insufficient, incorrectly assuming that the process decision maker is the security manager. In general, higher level executives act as risk treatment decision makers while security managers act at the point of treatment implementation. Due to its hierarchical standing, the security function often lacks awareness of broader organizational activities and context that affect the organization's risk appetite.

Security can achieve better influence through more explicit engagement with general manager level decision makers at key touch points during their assessments.

This study investigated 27 security, specialty risk, and general risk management standards and guidelines to identify common themes and limitations within the documented best practices. The study uncovered that the identification of the decision maker is not explicit in many of the models, a fact reinforced by participants who believed one of the weaknesses of the risk assessment process is the assumption that the decision maker is the security professionals themselves.

When considering the decision maker, guidelines such as OCTAVE and the ESRM model indicated that the key factors considered by senior management was their perception of what constituted a critical asset or what needed the most protection.

The analysis found that the ISO 22317 included the term "top management," however, the context was to communicate top priorities, and then approve results rather than as a decision-making capacity. Nevertheless, analysis showed that the detail behind these factors does little to explicitly encourage the risk assessor to identify the decision maker and align their message with their criteria and what they believe is critical

Study participants confirmed the findings, highlighting that in practice, while many of the models assume that the security professional is the decision maker until the selection of the treatment, security professionals are not the corporate decision makers—highlighted by a study participant who stated, "I like to talk about [security] risk management...as the process we're using to support your decision making. The decision maker is never security."

Participants noted that the decision maker for security risk management was often a senior executive outside of the security function; for most participants, security risk decision-making fell under the auspices of health and safety, facilities management, or operations. That is, organizational managers above or outside of the security function. Furthermore, it was found that in smaller companies the decision maker was often the head of finance. In the more risk-mature or compliance-based organizations, a chief risk officer or similar was the ultimate decision maker for security risk decisions.

However, the study found professionals in compliance driven (e.g., financial services, banking) or critical infrastructure environments (airports, nuclear energy plants) reported a degree of decision-making influence in terms of resource allocation. Still, they reported more senior approval was required over certain levels, often building assumed rejections and resubmissions into the plan. Many of the study participants believed the security risk management process is an information-gathering process from security followed by a decision-making process from a corporate manager or executive.

Many participants expressed that standards do not effectively specify that the decision maker is outside the SRM process, or the requirement for security managers to engage with them to establish the risk context. While they may acknowledge within the detail that the decision maker needs to be identified to allow contextually appropriate communication, it is not explicit within any of the models used, with very limited exceptions. The study concluded that there is an incorrect assumption that the decision-making process is part of the role of the risk assessment process owner, or the security manager, which it is not. Ultimately this results in the information being presented to the decision maker, oftentimes being incongruent with organizational objectives or requirements, meaning that the security position may be overlooked or rejected altogether.

Alberts, C., & Carnegie-Mellon University Software Engineering Institute. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* United States: Carnegie-Mellon University Software Engineering Institute,.

Allen, B., Loyear, R., & Noakes-Fry, K. (Eds.). (2017). *Enterprise Security Risk Management : Concepts and Applilcations.* Brooksfield: Rothstein Associates, Incorporated.

Funded by ASIS FOUNDATION

This is part of a series of nine short synopses, this paper explores the findings of an ASIS Foundation study conducted by Dr. Michael Coole, Nicola Lockhart and Jennifer Medbury of Edith Cowan University in Australia in 2022.