Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION™

FINDING FIVE:

SECURITY RISK DIAGNOSIS AND SECURITY RISK TREATMENT ARE NOT A SINGULAR ACTIVITY AND SHOULD BE PERFORMED AS SEPARATE DECISION PROCESSES

Most published risk standards steer assessors from assessment (diagnosis) to treatment identification and implementation. However, due to organizational structure and management level positioning, security is often not the corporate decision maker. Security often does not hold the authority required to effectively move into the treatment stage without prior approval from higher level managers who allocate financial resources. This often means that recommendations provided to the decision makers are based on assumptions of risk appetite, capability, and resource availability—economic decisions outside of the security department's remit.

This study investigated 27 security risk and general risk management standards and guidelines to identify common themes and limitations within the best practice. The identification and implementation of treatment strategies is structurally consistent across many of the various risk models and standards reviewed. Such consistent format implies treatment taking place before the risk review being presented to the decision maker.

Consequently, participants identified that while many of the models presented a cyclic approach, the absence of the interaction with the decision maker after the risk evaluation stage and before the risk mitigation or treatment stage made this process, in practice, inauthentic. Participants said security risk assessments are often being prepared and presented based on the judgement of the risk process owner based on the company's risk tolerance, appetite, and budget, which more often than not, is not part of the context, expertise, or authority of the security function (see Finding 4).

When asked about the disconnect between the risk identification communication and the communication of risk treatment, many of the participants stated that the model specifics are less important than the practitioner's ability to be flexible within this process and adapt as necessary, preferring to focus upon the importance of communicating in general and establishing the

context more effectively once the context and required language (value, impact, etc.) has been established. These findings are in contrast with the various published intelligence cycles. Within these models of practice, the assessor is designated to communicate their findings to the decision maker before receiving feedback and further direction. Participants noted that this distinction between communicating the identified risks and later identified treatments are two very different tasks.

Consequently, this study recommended using risk models that use distinct and separate messaging tools for the different stages of the process. For example, a business impact analysis for the risk identification, assessment, and evaluation stages; and a cost benefit analysis and decision comparison recommendation for the risk treatment identification process. This approach would mean models explicitly incorporate or acknowledge the need for higher level management decision making and direction to take place as part of the formal security risk management activity rather than missing key decision-making criteria and stages, delivering just the treatment suggestion message.

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.

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.