Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION™

FINDING EIGHT:

LANGUAGE IS A SIGNIFICANT ISSUE WHEN COMMUNICATING MESSAGES OF SECURITY RISK

The plethora of general and security-specific risk management models has resulted in a lack of clarity around risk terminology and language both across the industry but also at an organizational level, further impacting security's sphere of influence. Consequently, communication of the security risk message is a key factor in organizational influence, especially the ability to foresee, but more importantly understand (through such theories as psychometric dread) and effectively articulate (through such methods as business impact analysis) the risk impact to the organization. Focus groups showed the ability to communicate the link between the operational nature of security risk to comparable strategic business impacts were the most effective means of gaining influence. Security professionals can achieve better influence by translating security risks into business language, using business metrics for senior decision makers and boards. It was noted that it is not the role of boards to understand security, but security's role to communicate to the board.

Throughout the study, the issue of clarity of language was a consistent and significant theme. Most participants considered that the lack of linguistic clarity of numerous terms caused considerable confusion in achieving security risk influence. As one participant stated, defining some terms is a "horrendous problem," a "nightmare scenario," and "nonsensical to the people you're trying to influence." Some specific and significant miscommunications include:

- The understanding of security and the role it plays within an organization is oftentimes misconstrued; there is a requirement to delineate areas such as physical security, IT security, and cybersecurity.

- Participants raised several linguistic concerns that can have a dramatic impact on security risk influence. For example, cultural language issues, noting for example, the words for risk,

safety, and security in some countries are treated as the same concept.

- There is a significant language disconnect between the risk language used in private corporations and that used in government agencies. For example, according to one participant, "dumbing down" for the government agencies resulted in significant loss of original intent and important nuance.

- The specific notional distinctions between risk, threat, and intelligence—terms are often used interchangeably and incorrectly—were identified as a barrier to effective security risk influence. Participants suggested that misunderstanding of these key concepts often happened at the C-suite level, and given the lack of time generally assigned to the security team, it was often impossible to realign the definitions resulting in a dilution of the security risk message.

- Participants noted that stronger organizational risk language alignment and standardization within an enterprise risk management framework and in the analytical metrics used is key to achieving better risk message influence. Such alignment would enable more effective comparison of cross-organizational risk typologies. Participants said achieving this level of organizational embeddedness requires both higher level and broader general risk management training, which are often not expected, required, or desired by security managers. Again, the theme of broader management education for security managers was evident.

Poor communication of the risk message is a salient theme throughout the research. Specifically, clear communication significantly enhances influence, however, such communication currently is a key weakness of security professionals. Participants all agreed that "security must speak the language of the decision maker." Improvement in this area could make a drastic difference.

One key question is: Who is security communicating to? The ability to communicate directly to the requirements of the decision maker using the correct language and tools, is a key requirement. Yet all participants noted the lack of explicit requirement to identify the decision maker at the appropriate points in the process. Participants said current models advise communication and consultation with the decision maker at all points of the process is not helpful. Such guidance lacks any practical meaning because it is overly broad.

Another key question is: Why is security communicating a risk message? Translating the operational risk from a security threat assessment into comparable risk language that is understood and accessible by senior decision makers is a vital skill in ensuring that the security risk message is appreciated sufficiently to ensure appropriate resource allocation. As one participant stated:

> *The outputs of an effective security regime (that risks are lower as a result of all the great work security folk do!) need to be standardised as to other operational risk types for it to be valued. I also think physical security teams and leaders need to understand the top-down enterprise risk view and see where physical security sits and why. The language of operational risk, and ultimately enterprise risk, needs to be understood and built into the security frameworks for it to mesh, otherwise the board will not understand or value the input.*

Participants said for security managers and executives needed to understand and communicate the breadth of their purview across the organization to demonstrate that security risk is not actually siloed but has broader, strategic-level

impacts. While many of the participants recommended highlighting the impact and consequence factors across the entire organization and making security a "force-multiplier," they also understood that the language of the board is money, and importantly, value to the bottom line. Many of the participants agreed that the use of specific tools such as a business impact analysis is an effective method of communicating this, but many noted the use of these tools is not specified in the models, or if it was, it was buried deep within the explanatory notes that are often bypassed by busy security professionals who have not studied business and are thus unfamiliar with such tools. One participant observed:

Threats and dreads are often visible, visceral constructs... but often security threats, unless [they are] visceral or exciting, like terrorism or cyber breach, people can't relate. It's too abstract. And so therefore, what you're communicating and how you communicate my experience, policies, and procedures in the hands of more than two people are interpreted in different ways, which is why the metrics and observations and evidence that needs to be collected has to be far more rigorous..."

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.