Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION™

FINDING THREE:

ENTERPRISE SECURITY RISK MANAGEMENT IS NOT YET ACHIEVED

Security professionals expressed the view that the operational nature of security risk resulted in lower feelings of dread about security risks when compared to some other business risks. As a result, organizations reject security risks as enterprise-level risks. The exception is cybersecurity threats, which had a high dread factor among corporate executives, who in turn considered cyber threats as strategic-level risk. To overcome this, security professionals need to have clear understanding of the broader categories of organizational risk (risk taxonomy), including third-party risks, capital management, and government oversight concerns, and how security impacts and integrates with such risk concerns.

Both the literature review and participant responses suggested that the premise that security has influence across all corporate activity was a misnomer, in part due to the way organizations are hierarchically structured and how broader decisions are made. Re-acknowledging the idea of a technical specialist versus broader general manager, executive level participants reported that while they commenced their careers in security, they have moved above that role and are now general managers, with a much broader view of the organizational risk spectrum that they had not previously been aware of in their security role. As one executive stated:

"It's actually the assessment of the whole taxonomy that provides a hierarchy. I think security professionals, having been one myself, have a really limited tunnel view almost, looking up, but the board, their view downwards is really very different. My board is currently talking about third-party risk, compliance, capital management, governance and oversight, and cyber is in fifth place. Cyber isn't even top three, and all the security managers immediately think cyber is number one! … I think it's clear that although security

professionals can see the business context that they need to deliver security within, they might not see the risk context—it's this limitation that will mean security professionals will lack influence. When stacked up against other risk types, physical security is lower risk and therefore lower priority. And the big challenge is that unless security professionals talk the same language and use the same risk tools [or metrics] as the other risk types, then influence will be lacking. So, this notion of language and understanding of concepts around taxonomies, operational risk frameworks, and enterprise risk needs to be looked at closely."

The discussion on enterprise security risk management (ESRM) provided both mixed, and sobering results. For example, three participants—all of whom were corporate consultants, nonsecurity—pivoted the discussion to suggest that ESRM is a misnomer given that "security" as a concept is a mitigation strategy rather than a risk factor, and that an organizational enterprise risk management (ERM) strategy would only consider security as a treatment option. What became clear is the lack of consensus between practitioners and organizations on the role and importance of the security function. Indeed, the discussion was if security had a role at all or was merely "one tool in the risk mitigation toolbox."

One corporate executive (nonsecurity) provided examples of an organizational risk taxonomy, illustrating that within the broader organizational risk hierarchy, security risk featured in only three out of 36 business unit risk concerns. This discussion highlighted a lesser importance of security risk within the wider risk framework, and importantly, a distinct lack of widespread use of these tools such as a formalised risk taxonomy document or an ERM framework. When further questioned on the existence of an ESRM/ERM program or an organizational risk taxonomy, the significant majority of participants from noncritical infrastructure organizations stated that either a framework did not exist or, if one did exist, it was not communicated widely nor understood by the security and other operational business units.

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.