Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION

OVERVIEW AND RECOMMENDATIONS

The 2022 study investigated the complex issue of the level of influence that security risk management holds within the corporate context. Security risk management has a long history and broad acceptance as an essential organizational activity for achieving business objectives. However, the degree of decision-making influence achieved by security professionals is poorly understood, with many corporate security managers and executives anecdotally reporting low levels of corporate influence in managing security threats. Consequently, this study undertook a research-informed approach to the question of corporate security's current sphere of risk influence to establish an initial understanding of the influence security's risk message has across various organizations.

The study objectives were to identify professional barriers to achieving effective influence and uncover recommendations that may assist security professionals achieve stronger risk influence when advising corporate decision makers. Researchers anticipated that study participants would provide narratives expressing initial barriers encountered to influence, and how they overcame them to achieve robust influence. What emerged was a clear narrative that corporate security lacks influence outside of environments where security is mandated, and when security is legislatively mandated, it operates on a more compliance focus of practice rather than as a valued risk reduction business enabler. The study found that security risk management has a technically focused, narrow sphere of corporate risk influence, and uncovered key findings impacting security risk management influence, including the key requirement to identify, understand, and integrate into the organizational risk context.

RESEARCH APPROACH

This report is the result of a literature review of organizational management publications; a comparative analysis of risk management standards, guidelines, and instruments; and 11 focus groups where corporate professionals across the world provided insight into the findings based on their own experiences.

The literature review interrogated seminal management, socio-organizational and security and risk management texts to respond to the question: *What management theories are relevant to the positioning of corporate security within the organizational setting?* The literature review provided the framing for what security risk management should be according to seminal management theories.

The comparative analysis of the risk management standards, guidelines, and instruments investigated structural and thematic similarities and differences between the differing types of standards, allowing for a thorough understanding of how the standards work, their focus, and their application. Asking the question: *What is the current published approach to SRM?* and building upon the findings from the literature review, the review of the standards highlighted what best practice could be. However, the thematic analysis also revealed the limitations of these tools.

The 11 focus groups consisted of 25 international security and risk professionals and corporate executives. The professionals interviewed included past and present CEOs; CISOs; CFOs; CROs; facilities managers; security managers; project managers and consultants; security and nonsecurity consultants; and government engineering and security consultants drawn from around the world and from varying managerial echelons. The participants responded to questions developed through the previous research stages, ultimately responding to two questions: *What is the perceived corporate influence exerted by the SRM professional?* and *How can SRM more effectively influence corporate decision making?* The focus groups uncovered the experiences of industry professionals and organizational executives, identifying the disconnect between professional reality and best practice as described in the literature and professional standards. The focus groups compared, discussed, and analysed what security should be, what it could be, and what it actually is, highlighting the limitations and barriers to security risk influence as well as opportunities for enhancement.

KEY FINDINGS

FINDING ONE: ***THE SPECIALIST VERSUS THE GENERALIST***

Security is a technical, specialized activity, resulting in lower influence than broader generalist activity managers. As an area of technical specialized activity, security is considered a business enabler. This specialization means that at a corporate level, security has a constrained degree of influence when compared to general managers who work across multiple business activity areas and demonstrate higher degrees of business influence. While security's operational activities span the organization, its risk management diagnosis activities are siloed, therefore giving an impression of broader influence than it achieves at senior decision-making levels. The study found a disconnect between the literature and the industry perception of the organizational positioning and subsequent influence levels of organizational security.

FINDING TWO: ***ORGANIZATIONAL LEADERS SEE SECURITY AS AN OPERATIONAL RISK CONCERN, WITH LIMITED STRATEGIC IMPLICATIONS***

The study found that corporate risks considered by and under the influence of executives with broader influence than security have a higher

potential impact at the strategic levels of the organization, as do risks with a higher dread factor. Executives often see security as focused on the operational levels of risk impact. This means security professionals have less influence across broader corporate decision making, and places security lower in the organizational and risk hierarchy than other areas of risk concern. For security to have stronger weighting in their risk message they must communicate how security events impact the strategic objectives of the organization.

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.

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.

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.

FINDING SIX: ORGANIZATIONAL CONTEXT HAS A SIGNIFICANT IMPACT ON SECURITY'S RISK INFLUENCE

Influence is impacted by organizational context, notably when security resourcing and implementation is mandated within a compliance-directed, regulatory environment. For instance, personnel security vetting is accepted and standard practice because it is legislated and audited—there is a mandated and collective agreement on the importance, and therefore security influence. Focus group participants acknowledged that often security risk management does not form part of a regulatory framework, therefore the implementation of security programs within a self-directed environment result in security risks being prioritized behind compliance driven concerns, resulting in reduced influence.

FINDING SEVEN: SECURITY AS A BRAND LACKS PROFESSIONAL RESPECT, COMPARED TO TRADITIONAL PROFESSIONS

The study uncovered a perceived degree of professional disrespect for corporate security. Many participants acknowledged that security professionals often learn their business through policing or military careers, as opposed to formal university education. Participants noted that professional certification on its own does not engender, at senior levels, the same respect as formal university education. It was therefore expressed that fostering the security "pracademic" is a key to developing appropriate business skills and respect, coupled with security industry certification, practical experience, and individual expertise. While the research indicated this is changing, such change was seen at the individual level rather than culturally at the industry or sector levels, resulting in a perception of an educationally inferior profession.

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.

FINDING NINE: INFLUENCE IS IMPACTED BY CHARACTERISTICS OF THE INDIVIDUAL

Security, as an area of technical specialized activity, does not exert the degree of corporate influence experienced by other business areas of technical specialization such as law or accounting. However, individuals themselves can achieve very high levels of influence through personal leadership, where influence is best considered on a continuum and is a convergence of an individual's education and experience, personality facets including communication skills, and the organizational risk context in which they operate.

RECOMMENDATIONS

The findings led researchers to make four practical recommendations, designed to be actionable steps for security professionals to improve their organizational and risk comprehension and identify their limitations and barriers, then work within those constraints to change working practices to maximize organizational influence.

To achieve better corporate influence, security professionals should consider:

- Aligning their risk management work directly to the broader organizational risk hierarchical framework. For security professionals to clearly, concisely, and accurately inform decision makers about their risk message they need to ensure this message is aligned to the precise business risk context and communicate their findings in exacting and comparable business terms using business metrics. Security professionals should seek to understand the organizational risk taxonomy, formally published or otherwise. This approach will enable business leaders to fully comprehend and align all business unit assessments for comparable decision making.

- 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, 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.

- Engaging with renowned business schools and associations through membership and educational opportunities, to learn business metrics and language, while also communicating and embedding understandings of how security contributes to corporate success across all levels of business. It is only through such engagement that the benefits of enterprise security risk management can be communicated to and valued by general managers and boards.

- Embracing formal registries for members who hold recognised tertiary degree qualifications as a mandatory requisite. This approach would enhance and reinforce the status of registered security professional, overcoming disrespectful negative perceptions of educational inequality.

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.