THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

EXECUTIVE SUMMARY

ASIS FOUNDATION™

EXECUTIVE SUMMARY

The 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 gain an understanding of how security's risk message is received and acted upon across various organizations.

The study objectives were to identify profession barriers to achieving effective influence and to uncover recommendations that may assist security professionals achieve stronger risk influence when advising corporate decision makers. The researchers expected participants to provide narratives describing the initial barriers they encountered when trying to influence risk management decisions and how they overcame the barriers to achieve robust influence. Several security professionals shared such stories, but what emerged from the research is a clear narrative that corporate security lacks influence outside of environments where security is mandated. In situations where security is legislatively mandated, security operated with more of a 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. The researchers distill this narrow influence into nine key findings, and they recommend four ways the security profession can work to expand its influence and value.

KEY FINDINGS

SECURITY IS A TECHNICAL SPECIALIZED ACTIVITY, RESULTING IN LOWER INFLUENCE THAN BROADER GENERALIST ACTIVITY MANAGERS

Security is an area of technical specialized activity and is not considered as a business enabler. This specialization means 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. To enhance influence, security professionals must further develop business language and liaison skills and champion their risk message to those broader focused general managers who exercise higher decision authority.

SECURITY IS SEEN AS AN OPERATIONAL RISK CONCERN, WITH LIMITED STRATEGIC IMPLICATIONS

Corporate executives prioritize risks they see as having a higher potential impact at the strategic levels of the organization or that have a higher dread factor. This means security professionals have less influence across broader corporate decision making than areas considered to have broader, more strategic level impacts. This 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.

ENTERPRISE SECURITY RISK MANAGEMENT IS NOT YET ACHIEVED

Security professionals believe the operational nature of security risk keeps it from being an enterprise-level concern. Security risk is just one part of a broader operational risk portfolio. Cybersecurity risk is an exception, and companies treat it differently than other security risks because it has a high degree of dread factor among corporate executives, who see cybersecurity as a strategic imperative. To overcome this, security professionals need to have clear understanding of the broader categories of organizational risk—including third-party risks, capital management, and government oversight concerns—and how security integrates with such risk concerns.

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—including standards and related material—to facilitate their specific diagnostic tasks. The standards may acknowledge the need for executive buy-in, but their focus on broad processes overlooks the importance of, and provides little guidance in, how to identify, engage, and communicate directly with key decision makers. This contrasts with the corporate intelligence function and corresponding review of the intelligence cycle, which explicitly highlight clear focus on responding to a decision maker's requirements and producing products for decision makers. Security can achieve better influence by explicitly engaging general manager-level decision makers during their assessments.

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 purview. Security professionals may achieve better influence by accepting that messages of risk business impact and those of treatment cost benefit analysis are distinctly separate communication transactions.

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

Organizational context affects how much influence a function has, and this is noticeable when security resourcing and implementation is mandated within a compliance-directed, regulatory environment. For instance, security screening of personnel is an accepted and standard practice because it is legislated and audited—there is a mandated and collective agreement of the importance, and therefore security has significant influence. The research found that when security risk management is not mandated as part of a regulatory framework, which is usually the case, security managers often deemphasize security risk management while prioritizing compliance-driven actions. This further reduces the influence security has in an organization's risk management processes.

SECURITY AS A BRAND LACKS PROFESSIONAL RESPECT, COMPARED TO RADITIONAL PROFESSIONS

The study uncovered a perceived degree of professional disrespect for corporate security. Many participants acknowledged that often security professionals learn their business through policing or military careers, as opposed to formal university education. Formal university educational programs impart foundational business knowledge with prestige. Participants noted that professional certification on its own does not engender, at senior levels, the same respect as formal university education. The research indicates 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. Many participants engaged in this study acknowledged this is changing, however, the change is happening at an individual, case-by-case level rather than culturally at the industry or sector levels, resulting in a perception of an educationally inferior profession that must be overcome.

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 as well as 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 with importance placed upon the ability to foresee threats, 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. The ability to communicate the link between the operational nature of security risk to comparable strategic business impacts is 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. Research participants noted it is not a board's role to understand security, but security's role to communicate effectively to the board.

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. In this case the level of influence is a continuum dependent on an individual's education and experience, personality facets including communication skills, and the organizational risk context in which they operate.

RECOMMENDATIONS

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 their messages are aligned to precise business risk contexts and communicate their findings in exacting and comparable business terms using business metrics. This approach will enable business leaders to fully comprehend and align all business unit assessments for comparable decision making.

- **Using risk models with distinct and separate messaging tools for different stages of the process.** For example, use a business impact analysis for the risk identification, assessment, and evaluation stages; and use a cost benefit analysis and decision comparison recommendation for the risk treatment identification process. This approach would explicitly incorporate higher level management decision making input into the entire security risk management activity rather than only at the risk treatment phase.

- **Engaging with business schools and associations through membership and educational opportunities to learn how to communicate the importance of security and security risk management into traditional business metrics and language.** It is only through such engagement that the benefits of enterprise security risk management can be communicated, and influence achieved with general managers and boards.
- **Embracing formal registries for members who hold recognized tertiary degree qualifications as a mandatory requisite for top-level security positions.** This approach would enhance and reinforce the profession's status, helping to overcome the negative perception that security is a field of educational deficiency.

Project Findings: Limitations to Influence and Opportunities for Enhancement

Disconnect between the organizational seating of corporate security, and structure and direction of security risk Standards

LIMITATION/BARRIER TO INFLUENCE	OPPORTUNITY FOR ENHANCEMENT
Security is a siloed technical specialist activity reporting to a broader general manager and decision maker. Security lacks the decision-making and authoritative allocation of resources to effectively mitigate risk in line with published security risk management guidelines.	Security risk influence may be enhanced by corporate security executives and managers through pro-active engagement with their relevant general managers to ensure risk alignment with the broader corporate risk context and hierarchy.
While security's operational activities span the organization, its risk management diagnosis activities are siloed, therefore giving an impression of broader influence than it actually achieves at senior decision-making levels.	Security executives and managers must strive to understand the broader organizational context in which they operate in terms of both expectations and communication capabilities and methods. Then they can work to realign the security function so other executives understand security's risk management role. Revising the articulation of the position of the security function, realigning it with socio-organizational literature to provide a more realistic understanding.
SRM is perceived as a minor sub-set of operational risk management by organizational decision makers with no strategic importance in the risk hierarchy, thus having limited influence.	More effective communication of the strategic level impacts of security risk, using tools such as Business Impact Analysis. An embedded understanding of the organizational risk hierarchy through a formalized risk taxonomy would allow a more complete understanding of the organizational risk context, enabling better tailoring of the risk message. Security risk influence could be enhanced by formally separating operational and strategic risks into distinct risk evaluation activities, aligning assessments to broader organizational strategic risk taxonomy, profile and appetite.

Project Findings, *Continued*

The SRM Model authenticity in assuming that the decision maker is the risk assessment process owner

LIMITATION/BARRIER TO INFLUENCE	OPPORTUNITY FOR ENHANCEMENT
Current SRM models lack clear directive engagement with authoritative decision makers. The assumption by current models that Security makes the decision following risk identification means that the development of risk treatment plans without pre-engaging with corporate decision makers can lead to risk treatment strategies that may not align with the broader organizational strategic objectives, risk appetite or economic priorities.	The decision maker would be best placed to provide guidance and direction after the risk identification and communication activity, following clear business impact analysis. The SRM process should provide direction, cost/benefit-based treatment options in a format to aid decision-making.
Current risk models entwine risk treatment with risk identification, analysis, and communication, despite security's lack of decision authority. The presentation of this "complete package", omitting key tools such as Business Impact Analysis or cost/benefit analysis directed by the decision maker, results in the risk message being dismissed as being less relevant than or incomparable with other organizational risk messages.	The separation of risk assessment impact messaging and treatment option identification and cost benefit analysis into distinct formal business communication activities, returning to the decision maker at each stage to ensure next stage in process is best-fit. Risk messages should be communicated in a manner to enable direct business comparisons with other risk typologies across the organization

SRM Standards do not form part of a regulatory framework

LIMITATION/BARRIER TO INFLUENCE	OPPORTUNITY FOR ENHANCEMENT
Regulated industries have a compliance-based framework to which organizations must conform, consequently increasing organizational influence. The implementation of security programs within a self-directed environment results in security risks being prioritized behind compliance driven concerns and reduced influence.	Active engagement with lobbies or industry groups to develop and implement legislation – such as the United Kingdom's Protect Duty – designed to raise the requirement of considering security threats which pose a risk. Advocacy from oversight organizations, such as the Cyber Security Council, to create forums for private sector and government discourse on the corporate strategic value of security risk management.

Project Findings, *Continued*

Security as a brand - organizational perceptions

LIMITATION/BARRIER TO INFLUENCE	OPPORTUNITY FOR ENHANCEMENT
Security carries negative cost connotations, imparting limited business enabling capability.	Security risk influence could be enhanced through leveraging broader organizational relationships, working in partnership as opposed to siloes to become a "force multiplier" and business enabler.
Security management, and the profession in general, carries negative role connotations (guards, gates, guns) with senior organizational decision makers failing to understand the strategic importance of security.	Adopt case study analysis exemplars of both failures and successes (such as Rick Rescorla, In Amenas Gas Plant attack, Manchester Arena Bombing) as frameworks for communicating security risk impacts in amortized business terms, which enable comparisons of events between organizations who successfully mitigated risk through active security management and those who did not.
Security professionals are often ex-military or law enforcement with limited business experience or qualifications, often underpinned through vocational training and consequently lacking formal business education to be seen as corporate equals.	Develop professional partnerships with renowned international business organizations and schools to communicate and imbed understandings of how security contributes to corporate success at the strategic, tactical, and operational levels, and facilitate the embedding of ESRM thinking to general managers. Foster the role of the security "Pracademic" as a key to developing appropriate business skills, coupled with practical security experience and expertise. Formal registries of security professionals who hold recognized tertiary degree qualifications as a mandatory requisite. This approach would create the status of registered security professional towards overcoming disrespectful negative perceptions of educational inequality.

Language and Communication lacks clarity and consistency

LIMITATION/BARRIER TO INFLUENCE	OPPORTUNITY FOR ENHANCEMENT
Language and terminology used within SRM models lack connection with broader organizational risk and business language, impeding message transfer. This often means that the strategic impact of security risk is discounted by organizational decision makers.	Adopt broader business risk management analysis and communication techniques and language. Security risk influence could be enhanced using a formalized organizational risk taxonomy which standardized language of all risk types across the organization for direct impact comparisons.
Lack of clarity around language and concepts used across organizations, industries and countries, but also across various Standards. The subsequent confusion can result in a lack of comprehension at decision-making, resulting in the impact of the security risk message being diluted.	A review and adoption of general risk language as part of the oversight organization. At organizational level, an active alignment and "translation" exercise between external risk messaging and internal risk processes.

THE INFLUENCE OF SECURITY RISK MANAGEMENT:
Understanding Security's Corporate Sphere of Risk Influence

Principal Investigator: Dr. Michael Coole

Nicola Lockhart

Jennifer Medbury

Edith Cowan University, Perth, Western Australia