THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

ASIS FOUNDATION™

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

CONTENTS

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.

INTRODUCTION

As early as 1949, the influential industrialist Fayol acknowledged that security was one of the six main industrial business activities that all organizations require including manufacturing or production (Technical), the buying and selling of products (Commercial), the raising of capital (Financial), reconciling of balance sheets (Accounting), supervision functions of all managers (Administrative/Managerial) and the protection of assets (Security). The inclusion of security within main business activities supports the argument that security is an essential business requirement if organizations are going to successfully achieve their objectives despite being faced with various malicious threats.

Security's role in any business context is to manage the threats which pose a risk and is captured under the label of Security Risk Management. The requirement to manage corporate risk is well acknowledged, with the last decades giving rise to the increased role of Risk Management (RM) activities within organizations. Corporate security has embraced a RM approach, where such risk activities are facilitated using various tools formally published as Standards, which aim to assist in mitigating corporate risk. Such Standards provide "voluntary documents that set out specifications, procedures and guidelines that aim to ensure products, services and systems are safe, consistent and reliable" (Standards Australia, 2022, p. 57). Hopkin (2014) denoted RM standards as documents designed to "set out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework of activities supporting that process" (p.57). This approach has led to a significant amount of different risk centric standards, both general risk standards and more focused business risk concerns, including security risk management, crisis management, business continuity management, and more wide-ranging organizational resilience standards.

Published standards are considered cognitive models, aide memoires or frameworks developed to ensure that the assessor of security risk considers all practical factors and implications using an evidence-based process. The outcomes of risk management processes seek to steer or drive change, and to influence corporate decision-making to enable resources to be prioritised so that organizational objectives and functions can be pursued and undertaken within acceptable-risk tolerance levels (Coole & Brooks, 2021).

However, despite a plethora of such standards and the corporate acceptance of risk management activities as essential to business success, significant security events occur where forewarning was provided by the security function, yet prior risk messages were not heeded (see Case Study). Such a disconnect between specialist risk messaging and the resulting organizational behaviour indicates that a significant gap in corporate influence exists within the activity of security risk management. Such disconnect is historically captured by reflecting on the In Amenas Gas Plant attack of 2013 and by Statoil's own investigation into this terrorist attack, which concluded:

> *Security risk management processes do not follow through effectively from risk identification to action….security is generally not well understood within Statoil's leadership ranks, and as a result has not been prioritised, resourced or managed appropriately (Statoil, 2013, p. 5)*

This case study highlights that effective security risk management requires significant influence, defined as the ability to "cause someone

CASE STUDY: IN AMENAS GAS PLANT TERRORIST ATTACK, 16 JANUARY 2013

On 16th January 2013, a group of 29 Al-Qaeda linked terrorists stormed the foreign-run Tigantourine gas facility, detonating bombs and holding hostages for nearly three-days before the siege was ended by the Algerian military. A total of 39 expatriate workers and one local security guard were killed during the siege, resulting in multiple lawsuits from the victim families against BP, Statoil and Sonatrach. The estimated financial loss was over 12 billion US Dollars and operations at the plant (11% of Algeria's total natural gas output) did not resume full capacity for over three-years. In addition, there was considerable and sustained international media attention, resulting in immeasurable reputational damage to the companies involved and the region's gas industry.

A post event United Kingdom Coronial Inquest highlighted a lack of achieved influence by the security team, finding that on several occasions the on-site security function had requested numerous physical and operational security enhancements. There was also evidence that the on-site security professionals warned the executive teams of increasing internal security guard unrest, and the increasing external threat profile from active terrorist cells. Evidence also showed that risk assessment ratings given by the security professionals were overridden and ignored by on-site executives prior to the attack. Furthermore, the security professionals performed appropriate risk, threat and vulnerability assessments, and there was a concerted effort to communicate these risks; however, the risk message was not embraced nor acted upon by plant decision makers.

to change a behaviour, belief, or opinion, or to cause something to be changed" (The Cambridge Dictionary, 2022). Without such influence, security fails to achieve the impact it requires to secure an organization from harm. The concepts of influence, management and power are strongly entwined (Mintzberg, 1983, p. 4). For instance, Wong (2018) defined management and leadership as the "process of social influence which maximises the efforts of others towards the achievement of a goal". Various managerial theorists have seated influence within an organizational context as "where a person, group or organization triggers changes in the attitudes, values, behaviour, priorities and activities of others"(Pettinger, 2010, p. 172).

To date, broad but disparate research has been published discussing the influence exerted by security risk management activity within the corporate entity. For example, Borodzicz (2005, p. 153) called for more research into the ambiguous demarcation line between security risk and broader risk within an organization. This viewpoint was more recently reinforced by research published by Ludbey, Brooks, and Coole (2018) who noted a significant difference between the perceived role of the security risk manager according to the security literature, and the wider management literature. This lack in role and influence clarity has resulted in an inability to understand and articulate the limitations of security risk management and identify where opportunities exist for security risk managers to increase their degree of influence within their organizations. Noting such issues, investigating corporate security's sphere of risk influence can only be achieved from a sound basis in classical management theory.

RESEARCH METHODOLOGY

This report is the result of a literature review of organisational management publications, a comparative analysis of Risk Management Standards, Guidelines, and Instruments, and finally a

round of 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-organisational and security and risk management texts to respond to the question: *What management theories are relevant to the positioning of corporate security within the organisational 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. This stage responding to 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 comprised of 25 international security and risk professionals and corporate executives. The professionals interviewed comprised of past and present CEO's, CISO's, CFO's, CRO's, Facilities Managers, Security Managers, Project Managers and Consultants, Security and Non–Security Consultants, 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 lived experiences of industry professionals and organisational executives, identifying the disconnect between the literature, best practice through Standards and the professional reality, highlighting the limitations and barriers to risk influences, and the opportunities for enhancement. The focus groups compared, discussed and analysed what security *should* be, what it could be, and what it actually *is*.

REVIEW OF THE LITERATURE

THE ISSUE OF CORPORATE SECURITY AND RISK INFLUENCE

The broader management literature provides useful insights for security professionals in understanding their sphere of risk influence across corporate decision-making. For example, Standards Australia's Security Risk Management handbook states that the management of security risk "is a key and fundamental part of... wider risk management activities... [and] should be interlinked... with all other risk management activities" (Standards Australia, 2006, p. 3). However, despite such documents, Chase recognized, "business executives don't necessarily see the importance of security mitigation programs in helping them accomplish broader organizational goals" (2014, p. 45), and this results in lower levels of organizational influence. The formal integration of security into Enterprise Risk Management (ERM) processes, while a well published view and recommendation across the security literature, is in reality "rare and fleeting" further arguing that the hesitance of the security risk management function to adopt an organization centric view, preferring to "hold on to security as an age-old link to law enforcement" (Lefler, 2015). Lefler (2015, p.46) summarised that the security risk function will continue to operate in the margins "unless security leaders begin looking at themselves as business leaders and acting accordingly".

Allen et al. (2017, p. 5) also argued that "security is not viewed as an enterprise partner, risk manager and enabler of business operations, but is, instead, viewed as enforcer, rule-maker, task-doer, and (sadly) at times an obstruction to getting things done". Adding to this is the notion of a risk hierarchy, to which security is inconsistently positioned, but often, considered a lower risk concern when compared to other areas of corporate risk. This view is consistent with Ludbey and Brooks (2018) who found that whilst security managers deemed themselves to be high up in the organizational hierarchy (Stratum), they were in fact limited by their risk outlook based on timeframes in which they managed risk; with many security managers only managing shorter term (1 day to 5 years) operational risk, as opposed to longer term (5 years to 25 years) strategic risk concerns.

From a historical context, Dionne (2013) highlighted that broader corporate risk evolved from a focus on pure risk, mitigating very defined losses through early insurance schemes, through to a speculative risk management focus. Where such widening of the risk comprehension at an organization level sought to facilitate the undertaking of uninsurable speculative risk activities with potentially significant gains. Such broadening saw earlier conceptualisations of risk management merge into Enterprise Risk Management – defined as a corporate-wide integration tool that could increase value, letting an organization actively profit from different forms of risk coverage.

Acknowledging such a broadening in risk focus, Allen, Loyear, and Noakes-Fry (2017) aligned security risk management into this framework, defining Enterprise Security Risk Management (ESRM) as a comprehensive, holistic and all-encompassing approach to the application of fundamental risk principles to manage all security risks within an organization. However, security's influences and impact in the speculative risk environment and subsequently enterprise risk environment in corporate decision-making is poorly understood, meaning barriers in corporate security influence and opportunities for enhanced functionality are opaque. Corporate security's sphere of risk influence is seated within and impacted by the wider organizational context. Consequently, to develop deeper insights

into this complex problem, it is necessary to consider corporate security within the sphere of wider classical management theory, including organizational structure, hierarchy, and managerial stratum.

MANAGEMENT LITERATURE AND CORPORATE INFLUENCE STREAMS

Power is defined as the ability to exercise influence to effect outcomes, and authority is the legitimisation of such power to exercise this influence (Mintzberg, 1983; Pettinger, 2010). In the corporate domain, power is derived from organizational hierarchy and from 'spheres of influence (Pettinger, 2010, p. 193). Simons (2005) argued that the span (sphere) of influence was one of the four key pillars to the success of organizational role design, alongside control, accountability and support. Simons included a quote from the CEO of Proctor and Gamble, in which the "measure of a powerful person is that their circle of influence is greater than their circle of control" (2005, p. 6).

For security professionals, it is important to note that two distinct streams of organizational executive influence emerge from this literature:

- Stream One, comprising executives who have a specific focussed specialization (technical expertise), and
- Stream Two, those executives who have a broader, cross functional purpose across the organization.

According to Simons (2005) Stream Two executives have a wider sphere of organizational influence that Stream One, due to their requirement to work across multiple organizational silos and influence more diverse departments; directly attributing span or sphere of influence with the level or difficulty of the role (p. 6). In contrast, Stream One executive being of a specific technical focus have a more limited (Siloed) sphere or span of influence. Such a distinction is important for security risk management as the classical management literature places corporate security as a specialized activity, seated in what is termed the techno-structure of an organization and providing expert technical advice (Stream One). Consequently, this may explain why security in many corporate contexts has, or appears to have, a more limited sphere of risk influence compared to those Stream Two executives who have a broader, cross functional decision-making and authority.

ORGANIZATIONAL ACTIVITY, STRUCTURE AND HIERARCHY

Many security professionals may not have formally studied classical management theory. However, to understand barriers to corporate security influence, it is necessary to understand what the management literature states, and therefore how general managers from backgrounds other than security are focused. A notable early management theorist was Fayol (1916) who placed significant emphasis on the importance of broader administrative or managerial skills over focused technical expertise in achieving core organizational objectives, stating:

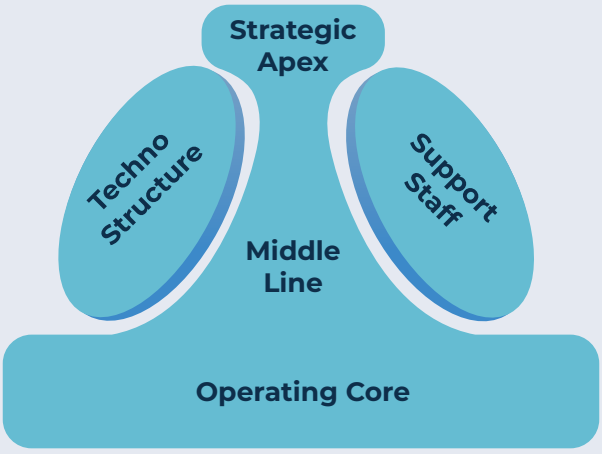
> *The result is that the time given to technical questions is progressively reduced, and becomes almost negligible when we reach the level of the head of a really big concern…it is certain that a leader who is a good administrator but technically mediocre is generally much more useful to the enterprise than if he were a brilliant technician but a mediocre administrator (Fayol, 1930, pp. 79-81)*

Fayol's work specifically focused upon broader management skills and a top-down approach to

organizational management and decision-making to achieve core objectives. This approach formed the basis of early Administrative Theory, a frame of thinking still relevant today. This thinking is consistent with a chain of command approach to management (Wren, Bedeian, & Breeze, 2002). The work of Ludbey and Brooks (2017) highlighted a link from this body of classical management theory to contemporary corporate security, noting that goals of organizations are only achieved through hierarchical structuring and that it is commonly accepted in line with key historical classic management theorists including Mintzberg (1980) and Jacques (1996) that this is the hierarchical division (stratification) of organizational work.

Ludbey and Brooks (2017) argued that corporate security is located within the techno-structure (Figure 1) as a facilitator of core activities, as opposed to the operating core which achieves the core business of an organization. The argument that security represents a technically specialist service within an organization, and therefore separate from the operating core, was inferred by Sennewald (2011, p. 27).

Figure 1: **Mintzberg's Abstracted Organizational Structure** (Mintzberg, 1980)



This earlier work provided grounding to Ludbey and Brooks' (2017) findings that security is a specialized activity within an organization, providing protective services seated as per Mintzberg (1980), in the technical specialist component of the organizational structure. Such a view reinforces that corporate security managers are considered as Stream One, under Simons' (2005) model, and consequently would not wield the same degree of organizational influence as their Stream Two, generalist counterparts who work across multiple organizational silos across diverse departments.

Adding to this discussion is the classical work of Jaques', whose Requisite Organization Theory (1989) states that an organization should be structured so that there are distinct managerial roles and that the 'task complexity' at each level is correctly aligned with the individual's personal capability (Jacques, 1989; Kleiner, 2001). Jacques' management hierarchy includes seven distinct strata:

Stratum 1 – team member; conducts the operational work

Stratum 2 – front line supervisors; makes sure the work gets done

Stratum 3 – contract or section manager; single serial systems

Stratum 4 – senior contract or section manager; multiple parallel systems

Stratum 5 – contract or section director; strategic vision

Stratum 6 & 7 – executive and board

Ludbey and Brooks (2016) applied Jacques' model to the contemporary corporate security domain and noted it consisting of more defined, technically specific, and operational

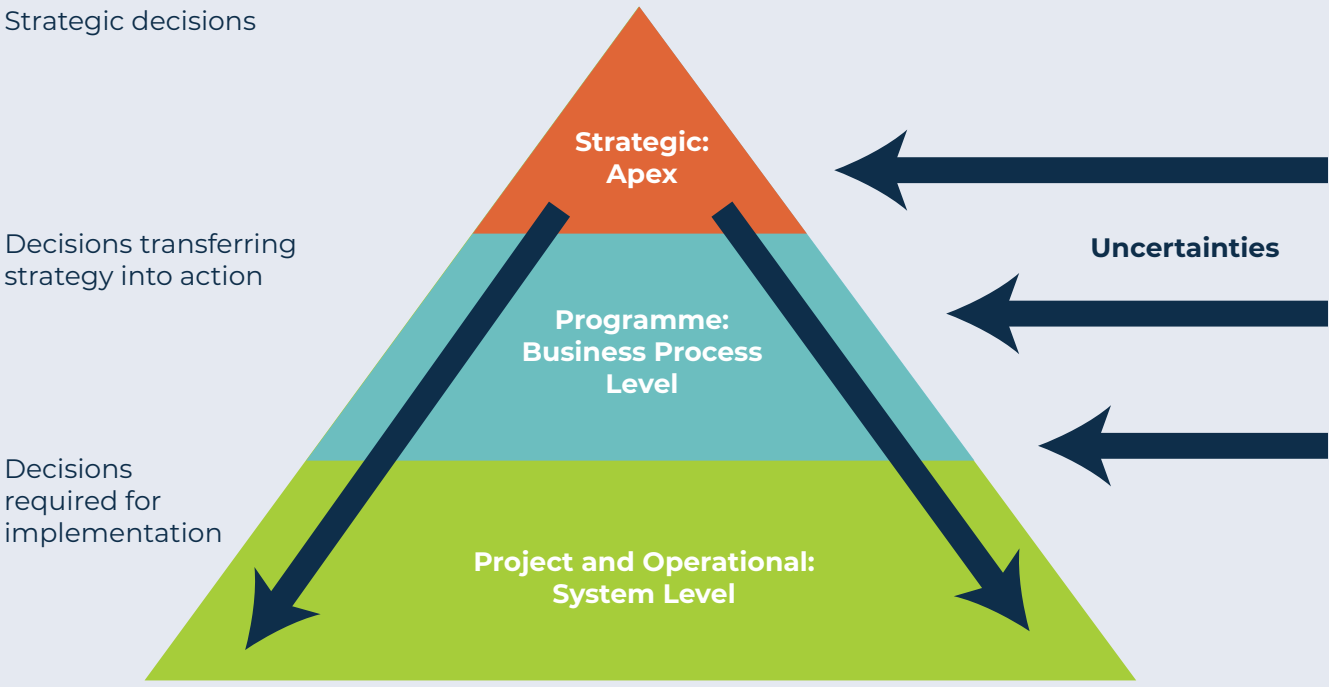
security roles at the lower end of the stratum. As tasks become more abstract and of a governance focus, they moved upwards through the stratum of management (Mintzberg, 1979; Brooks & Corkhill, 2014; Ludbey et al., 2018). These combined bodies of work highlight that organizational influence directly relates to both hierarchy and position within the organizational structure.

RISK HIERARCHY AND CORPORATE INFLUENCE

Classic management theory provides a frame of thinking that considers that not all managers sit at the same level of authority (Hierarchy), and that the division of work is based on the degree of business focus between highly focused technical work and broader business focus managerial work. This same body of literature also established the idea of a risk hierarchy or stratum, acknowledging that not all risks have the same impact concern for an organization.

The existence and practical application of different types of risk within an organization is acknowledged in various Standards including the ASIS International Risk Assessment Standard (ASIS International, 2015, p. 48); however, there is limited articulation or understanding of a hierar-

Figure 2: **Organizational Risk Hierarchy Adapted From UK Government Strategy Unit** (2002) **and NIST Risk Management Framework** (2012)



chical application of risk within an organization across security texts. Notwithstanding this gap, governmental bodies have formally recognized the existence and importance of a risk hierarchy in the practical application and management of their security risks. For example, following the events of September 11, 2001, the United Kingdom Government commissioned a report investigating how to improve their security and general risk management processes (Strategy Unit, 2002). This report found that the Government was required to manage risk at three distinct levels (Figure 2):

- Strategic
- Programme (including procurement, establishing projects and business continuity)
- Operational (including technical issues and managing resources)

Consequently, guidelines were formally published that led a codified stratum or hierarchy of risk under the guise of The OCEG Orange Book guidelines. The acceptance of this Hierarchy of Risk is also found in the National Institutes of Standards and Technology (NIST) Risk Management Framework used by the US Government in identifying Information Technology Risks (Figure 3) (National Institute of Standards and Technology, 2012).

A critical review of this security risk management and broader risk management Standards literature highlights a disconnect between the expected risk influence of corporate security risk management and the broader management risk literature. For example, ASIS International (2015) defines security risk management as having an "enterprise-wide strategic" role within the organization. However, in contrast, the NIST Standard and OCEG Orange Book specifically indicates that this is not the case given the specialist and operational focussed nature of security risk. Such a functional and cultural organizational disconnect was earlier recognized by Briggs and Edwards (2006):

The impact of the security department is proportionate to its ability to persuade individuals and teams all over the company to collaborate and cooperate…formal security training can tend to be risk averse, while businesses need to take calculated risks to stay ahead of competitors.

UNDERSTANDING SECURITY RISK MANAGEMENT

ASIS International highlight the importance of the Security Risk Management process in supporting "enterprise-wide strategic and operational activities, as well as program and project-related activities" (2015). These contemporary moves towards Enterprise Security Risk Management (ESRM) highlights the importance of integrating "the fundamental risk principles to manage all security risks – whether related to information, cyber, physical security, asset management, or business continuity" (Allen et al., 2017, p. 4). ESRM represents a theoretical cultural shift away from the traditional idea of pure risk management (loss avoidance), towards recognition that the security function does contribute towards speculative risk management activities of the organization. Chase (2014, p.8) asserted that for the security risk professional to be able to exert influence with other business units and decision makers at more senior levels, participation in an integrated ESRM management model is a key requisite.

SECURITY RISK MANAGEMENT STANDARDS: A COGNITIVE MODEL

Best practice in security is achieved through employing a systematic approach using diagnosis (security risk), inference (security theories

and principles) and treatment (operational controls) modalities. Accurate threat and risk assessments are the key to a strong security diagnosis defined as "the cognitive task associated with assembling a client's needs or articulating the problem" (Abbott, 1988; Coole & Brooks, 2021).

Risk is defined as the effect of uncertainty on objectives of that organization; therefore, the use of risk management models supports the user to objectively view the situation, make assessments based on pre-determined metrics and mitigate cognitive bias as far as practically possible. Whilst it is widely accepted that risk management models, which have been produced in the format of Risk Management Standards, are useful tools, it is important to acknowledge the limitations of such models. Such a limitation can be explained through the "The Unknown Unknowns". In 2002, Donald Rumsfeld gave the following response when questioned about the lack of evidence of the existence of weapons of mass destruction in Iraq:

> *There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know.*

Rumsfeld drew on a cognitive psychological technique known as the Johari Window to highlight that as humans, there are unknown risks arising from situations so unexpected that they would not be considered. This technique highlights that the use of such cognitive risk models is limited as we are unable to comprehend all possibilities. Furthermore, as approximations of a cognitive process, models are often limited to the most common occurrences of the process being modelled, and often, some details may be left out.

RISK DECISION-MAKING WITHIN ORGANIZATIONS AND THE LIMITATIONS OF STANDARDS

Risk-related decision-making can be denoted as decisions that will influence a system or organization either by increasing or decreasing the risk (Zhu, Haugen, & Liu, 2021). Zhu (2021) highlighted that risk related decisions vary significantly depending upon factors such as system diversity, product or system life cycle, incident prevention, consequence mitigation, impacts, object and time span. There have been many studies into factors taken into account when making risk decisions, including cognitive biases (Kinsey, Gwynne, Kuligowski, & Kinateder, 2018), past experience and individual beliefs, as well as environment, socioeconomic status, technology, politics, communications, market cost, reputation and social responsibility (Juliusson, Karlsson, & Gärling, 2005). Juliusson, Karlsson and Garling (2005) also found that organizational leaders made decisions based on their escalation of commitment and sunk outcomes – meaning they invest larger amounts of time, money and resources into a decision to which they have already committed; or "how far in the hole" they feel.

The most prominent approach to risk-based decision-making is the Von-Neumann-Morgenstein utility which states that a rational decision maker, when faced with probabilistic (risky) outcomes of differing choices, will behave as if they are maximising the expected value – in short, risks can be numerically ranked and then a judgement made upon this ranking. As a result, this formulaic approach makes up the basis of the risk assessment process. However, this approach has been criticised, with Poppe (2016) arguing that organizational leadership rarely acquiesce the big risk decisions to a formula, preferring to "do a gut check", or use a combination of the recognition-primed decision-making, sense-making and intuition decision-making

processes. Such an approach is consistent with the earlier work of Sum (2015) who found that despite Standards and guidelines in the risk management arena, decision-making tended to be more informal and based on intuition. It follows therefore that the risk assessment and analysis process, based on formulaic bounded rational decision-making, is only one tool, forming one part of the decision-making toolkit, where corporate decision-making requires the acceptance of a range of possible outcomes or consequences.

The way in which corporate decisions are made may therefore impact how security influence is achieved or not achieved. Consequently, how the risk message is communicated in relation to the decision-making paradigm needs to be understood. This understanding is important if security is to increase the sphere of risk influence across the broader organization, projecting beyond its technical seating. Such a point can be directly extracted from Malone's (2015) articulation of the intelligence cycle as a means of enhancing decision-making, where the threat assessment forms a key product in guiding organizational decision-making based on the accurately targeted audience.

REVIEW OF LITERATURE FINDINGS

The review of literature highlighted numerous insights for corporate security managers. These insights include evidence that the security function does not sit broadly across the enterprise as considered in some seminal texts and guidelines. In contrast to security's beliefs, the broader management literature sees corporate security as a specialist activity, seated within the technostructure as a corporate enabler, underpinned by, and focused on specialized knowledge and skill. Furthermore, security risk management is considered in the literature, including publications such as OCEG and NIST, as lower strata operational level risk management activity. Consequently, such a siloed remit reduces a security manager's influence across the broader organization, resulting in a reduced impact in corporate decision-making, despite a clear and consistent focus on protecting the organization's objectives from harm.

SYSTEMATIC REVIEW OF RISK MANAGEMENT STANDARDS

The systematic standards review investigated "*what the current published approach to risk management is*". This stage analysed the current documented best practice approach to security risk management using the qualitative research techniques of content, thematic and structural analysis.

The analysis uncovered a plethora of interconnected and overlapping Standards; for example, the ISO 22380 Family of Standards; the ISO 22300 Family of Standards and the ISO 28000 Family of Standards. Across these, the user was directed to risk assessment models and techniques from various other sources including ISO 31000 and ISO 22301. An indicative observation drawn was that such a plethora of documents may impede best practice in SRM due to such diversity in approaches. Therefore, the initial stage of this review identified and separated the various standards into Primary SRM Standards, Secondary or Specialized RM Standards and General RM Standards.

PRIMARY SECURITY RISK MANAGEMENT STANDARDS, GUIDELINES, AND INSTRUMENTS

These documents (Table 1) specifically sought to facilitate the identification, analysis, treatment and communication of security risks for the primary task of SRM within the context of criminogenic drivers (e.g. fraud prevention). The intent of these Standards was prevention-based security measures.

SECONDARY OR SPECIALIZED RISK MANAGEMENT STANDARDS, GUIDELINES, AND INSTRUMENTS

Secondary or Specialized Standards (Table 2) are documents such as Standards Australia HB 221: 2004 Business Continuity Management, to which the identification of security risks forms part of the process content and structure.

Table 1: **Primary Security Risk Management Standards, Guidelines, and Instruments**

INSTRUMENT NUMBER/NAME
Carnegie Mellon Operationally Critical Threat, Asset and Vulnerability Evaluation Framework (OCTAVE) (2001)
ANSI ASIS RIMS Risk Assessment (2005)
HB 167:2006 Security Risk Management (2006)
SRMBOK – Security Risk Management Body of Knowledge (2009) – Talbot & Jakeman
DHS RMF - Risk Management Fundamentals: Homeland Security Risk Management Doctrine (2011)
NIST RMF SP800-30:2012 Guide for Conducting Risk Assessments (2012)
ISO 27005:2012 Information Technology – Security Techniques – Information Security Risk Management (2012)
ASIS ESRM - Enterprise Security Risk Management Guideline (ASIS ESRM) (2019)
ISO 22380:2020 Security and Resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures (2020)
CISA Interagency Security Committee Risk Management Process (2021)
CPNI Role-Based Protective Security Risk Assessment Guidance (2022)

Table 2: **Secondary or Specialized Risk Management Standards, Guidelines, and Instruments**

INSTRUMENT NUMBER/NAME	STANDARD FAMILY
HB 221:2004 Business Continuity Management Handbook (2004)	ISO 31000 Standard Family
HB 292:2006 A Practitioners Guide to Business Continuity Management (2006)	
ASIS SPC.1 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirement with Guidance for Use (2009)	
Information Risk Assessment Methodology 2 (IRAM) (2017)	
ISO 22384:2020 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish and monitor a protection plan and its implementation (2020)	
AS ISO 22301:2020 Security & Resilience – Business Continuity Management Systems (2020)	ISO 22300 Standard Family
ISO 22317:2021 Security & Resilience — Business Continuity Management Systems — Guidelines for Business Impact Analysts (2021)	
ISO 22331:2022 Security and resilience — Business Continuity Management Systems — Guidelines for Business Continuity Strategy (2022)	
AS 4811: 2022 Employment Screening (2022)	
European Union Agency for Network and Information Security (ENISA) Risk Management/Risk Assessment (RM/RA) Framework (2022)	
NIST Special Publication (Sp) 800-53a, Assessing Security and Privacy Controls in Information Systems and Organizations (2022)	

GENERAL RISK MANAGEMENT STANDARDS, GUIDELINES, AND INSTRUMENTS

General RM Standards, Guidelines and Instruments (Table 3) including ISO 31000 and COSO ERM were those documents which sought to facilitate the identification, analysis, treatment, and communication of risk as part of a broader risk mitigation objective.

ANALYSIS OF STANDARDS, GUIDELINES & INSTRUMENTS

The Standards were subjected to a comparative content analysis to review the similarities and differences between primary, secondary and general RM Standards; a thematic content analysis of all combined standards, and finally, a structural review of all the Standard models to identify and analyse processes and procedures.

COMPARATIVE CONTENT ANALYSIS

Evaluating the grouped Standards provided an insight into the focus of these risk areas (security risk management, specialized risk management and general risk management) and how the documents are applied within the risk management process. Several observations were uncovered which directly supported the notion of a risk hierarchy as evidenced in the review of literature.

The Primary SRM Standards focus on process management of operational risk.

The conceptual tasks of information collection and assessment take priority over both threat and risk elements within the primary SRM Standards; these security Standards are focused on the process of risk assessment and the associated tools. In support of this, the word cloud shows that within the top 30 themes within the primary SRM Standards, assessment techniques and terms referring to the processes feature most prominently. For example: "Analysis" (ranked 11th, 0.39%), "Likelihood" (ranked 13th, 0.33%), "Impact" (ranked 19th, 0.30%), "Vulnerability" (ranked 30th, 0.23%), and "Critical" (ranked 35th, 0.21%). The analysis shows that the primary SRM Standards are process focussed with limited consideration of the wider context within which SRM sits. The more limited focus on the wider organizational context is consistent with the notion of risk and organizational hierarchy articulated by Simons (2005, p.6) whereby the security activity sits with-in the technostructure focusing on their spe-cialization and operational risk, resulting in less organizational influence.

Secondary/Specialized RM Standards focus on compliance.

Of the secondary/specialized Standards reviewed, only two of the 14 Standards were authored by a private body, with the majority (86%) written by a government body or the International Standards Organization (ISO). Comparatively, 67% of the primary SRM Standards and 40% of the general Standards, were written by Government bodies or the ISO.

The main themes identified for the secondary/specialized Standards and guidelines includ-ed a focus towards industry/discipline specific elements including e.g., "Building", "Business Continuity Management (BCM)". Across the secondary sources, themes of "Standards", "Governance", "Government", "Stakeholders", "Review" and "Purpose", emerged, suggesting that these guidelines, whilst more content specific in nature, looked towards and answered to an external authority more strongly than the primary SRM Standards. On first review, this is inconsistent with the notion of risk hierarchy (and indeed organizational hierarchy) which suggests that further specialization and focus would reduce the consideration given to wider organizational requirements. However, it can be argued that a focus on compliance to rules and regulations imposed through Standards, legislation and audit is a narrower field of view, and the focus is on adhering to the boundaries placed upon it by the organization.

General RM Standards have a broader organizational focus.

The analysis demonstrated that for general RM Standards the term "Security" is not within the top 100 themes. Such a position suggests that the element of security is not considered a main risk concern when managing broader organizational risk. This contrasts with Fayol identifying security as being a key organizational activity for success.

Consistent with the notion of a Risk Hierarchy, the general RM Standards are more heavily focussed upon the objectives, performance and compliance of the organization, within a business and organizational context. The general RM Standards assert the notion that the risk management process should form a business support function with the central concern being the organization itself rather than any specific process. The importance of "Management" is higher in the general RM Standards, with a weighting of 2.04% compared to a weighting of 1.3% in secondary/specialized Standards and 1.22% in primary SRM Standards. This suggests that the broader general RM Standards focus upon the management of the organization in broader terms, the secondary/specialized Standards manage their response to external rules and governance through compliance, whereas it

appears that the primary SRM Standards focus on the process itself rather than its role across the broader organization.

THEMATIC CONTENT ANALYSIS OF COMBINED RISK MANAGEMENT STANDARDS

The combined documents were subject to a thematic content analysis to uncover, analyse and report upon recurrent themes or topics. This was conducted using word counts (Table 4), and word clouds (Figure 3). Highlighting the top 50 words from all the Standards combined, the word cloud analysis (Figure 3) presents the most frequent terms at the centre, in the largest font size and brightest colour. Then, subsequent, less frequent terms appear around this salient term using a font size, colour intensity and location based on weighted percentage.

Numerous themes emerged from this analysis process:

The management of risk forms a key role in organizational objectives

The analysis from the combined Standards showed that the two most common terms are "Risk" and "Management". "Risk" appears at the top of the most frequent themes, highlighting that across all Standards, guidelines and instruments the overarching concept is risk, acknowledging the task focus of these documents. The importance of "Management" supports the literature and the notion that risk, and the management thereof, forms a key role in the successful attainment of organizational objectives. As per Fayol's works, the act of "management" as an administrative function for all managers should be integrated into all levels or organizational hierarchy and activity.

Risk management is a process of managerial control

Further investigating Fayol's managerial functions, the analysis uncovered that only one managerial function (Control) appeared in the top 100-word frequency list for the combined Standards. "Control" was ranked 22nd with a weighting of 0.25%. The presence of "control" so high in the analysis suggests that a core managerial element of risk management is the concept of control. Fayol (1949) defined managerial control as "verifying whether everything occurs in conformity with the plan adopted, the instructions issued and principles established" (p.107). Consequently, implying that risk management should be a top-down process, dictated to, managed by, and verified from above.

"Controls" as risk treatments vs. "Control" as a managerial function

While investigating "Control" as a managerial function, the concept of "Controls" as treatment strategies also appeared high on the count analysis (ranked 18th, 0.28% weighting). This conceptual term directly related to the notion of treatments, system variables put in place to control evaluated

Table 4: **Top 10 Word Frequency Count - Combined Standards**

WORD	WEIGHT %
Risk	3.20%
Management	1.53%
Security	1.24%
Information	1.15%
Organization	0.92%
Assessment	0.90%
Process	0.60%
Business	0.55%
Threat	0.50%
Objectives	0.43%

Table 3: **Word Cloud - Combined Standards**

risks. "Controls" as a treatment strategy appeared higher than the notion of managerial "Control". Consequently, "Control" and "Controls" as key concepts in security risk management were distinct. The term "Controls" as a treatment appears within the combined Standards more than the term "Control" as a managerial activity, emphasising a treatment component over the managerial component. This suggests that risk management tools are more concerned with the provision of a treatment strategy rather than directing managerial control from above.

Linguistic clarity is a significant issue

Further analysis show a mix of references within all Standards as to the definition and use of various terms; in some Standards, the term "Controls" referred to physical elements such as fences and access control systems, etc., often used synonymously with treatment. In the general RM Standards, the term "Controls" was used to reference auditing processes. Whilst investigating the context within which "Controls" was used, it was noted that HB167 directly referenced the language issues, designating it a "trap" (Standards Australia, 2006, p. 83).

Acknowledging the "confusion over the term 'controls', 'treatments' and 'countermeasures'... factors that may increase or decrease a risk can be regarded as controls" however goes on to state that 'controls' are used to specifically describe those factors already present and factored into the risk analysis. 'Treatments' are those controls that are to be introduced to improve the management of the risk following risk assessment". In those two sentences, it is perhaps ironic that the term "Controls" is used in multiple ways whilst trying to provide an element of clarity, adding another layer of confusion; at this point, control/controls could refer to managerial processes, current control factors in place, or future proposed mitigation treatment strategies. Of note, even in acknowledging this difficulty, HB167 does not address the lack of clarity suggesting "it is sometimes useful considering using them in different contexts".

Security *should* form a key part of organizational risk management

The term "Security" was the third most frequent theme in the combined Standards, highlighting the role of the discipline within the overall risk management process across an organization. Such a notion is not a new understanding, it is well supported by Griffiths et. al (2010) who stated that SRM forms a key part of an organization-wide approach to managing risk. This view is further acknowledged and formalised in Standards Australia's Security Risk Management handbook, which states that the management of security risk "is a key and fundamental part of... wider risk management activities... [and] should be interlinked... with all other risk management activities". Furthermore, the broader notion of ESRM also acknowledges this point, arguing security should play a central and integrated role in the broader organizational risk management process.

Fayol (1916) also identified security as a main organizational business activity, necessary for all organizations to be successful. Consequently, corporate security is formally acknowledged as an activity necessary for organizations to succeed. However, whilst this is acknowledged across the business and risk management literature and enshrined in the notion of ESRM and various supporting Standards, a significant published disconnect emerges. That is, security is a technical-specialist activity, which according to Mintzberg (1980), sits in the technostructure, outside the central management system or strategic apex. Such positioning means corporate security has limited, or no role with driving the business centric operational direction (Mintzberg, 1979; Martin & Fellenz, 2010), and according to Simons (2005), has limited organizational influence.

Risk management is process focused

The word count analysis showed the primary focus of the combined Standards was towards the identification (process-related terms) of the risk management process, with words such as "Information", "Assessment" and "Process" appearing closer to the middle. Whereas terms such as "Communication" and "Strategy" and "Plans" appeared towards the outer edges indicating they are less prevalent within the Standards. This analytical outcome was consistent with count analysis weighting list, which showed many of the terms that aligned to risk analysis and evaluation appeared less often. For example, the words "Criteria" ranked 46th with a weighting of 0.18%, "Communication" ranked 75th with a weighting of 0.14%, "Monitoring" ranked 78th with a weighting of 0.14% and "Capability" ranked 83rd with a weighting of 0.13%. With identification related terms such as "Assessment" ranked 6th with a weighting of 0.97%, "Analysis" ranked 14th with a weighting of 0.34% and "Identify" ranked 20th with a weighting of 0.28%, all appearing towards the top of the list, suggesting that the Standards are used primarily as a management direction and risk identification tool.

SRM is an information gathering exercise for the decision maker

"Decision" appeared in the top 20 terms within all the Standards combined with a weighting of 0.32%. An outcome that appeared to embed the decision maker in the risk process. However, further analysis ascertained that the decision maker was discussed most often in the primary security risk management standards. References were researched and coded, uncovering that most references to "Decision(s)", (totalling 88% of the references) were regarding the mechanics of decision-making process and using the assessment to inform and improve that process. It was also discussed in detail in terms of actions required should the risk assessments be rejected.

Of note, within the primary security risk management standards, the DHS RMF highlighted that the decisions and resource allocation was made by the Executives, and that the program planners (the risk assessment process owner) implement those executive decisions. The CISA ISC detailed the characteristics of the decision maker; ANSI ASIS RIMS Risk Assessment highlights that "the risk assessment provides assurance to decision makers" (p.8) and "provides input to decision-making processes" (p.19) and suggests there are "Management and decision-making requirements" (p.20). This analysis suggests that the decision maker is not only external to the security risk process, but is an executive or more senior manager, highlighting that ultimately security risk management decisions are made by management higher in the organization stratum, and the security risk management process is an information gathering tool to support this process.

The ANSI ASIS RIMS Risk Assessment dedicates an entire section to highlighting the importance of selecting the correct assessment techniques to align with the decision maker and that they should have appropriate authority. Such an outcome was observed in HB167, which discusses in depth the decision-making process alluding that the assessment message delivery needs to be tailored to the decision maker (p. 22). ISO 31000 discusses the communication and consultation process being used to influence the decision maker (p. 4), stating that the decision maker can be a stakeholder. This analysis showed that all Standards reviewed, noted, and discussed the decision-making process, highlighting the decision maker as being central to the process. However, investigation into the full Standards showed that the identification of the decision maker is implied in the "Establish the Context" stage rather than an explicit discussion or instruction. Only The Orange Book made specific reference to the need to designate or identify the specific decision maker (p. 26).

Communication is not as integral to the RM process as expected.

The role of communication in the risk management process was identified as significantly important during the initial background review. However, "Communication" ranked 74th with a weighting of 0.14%, highlighting that communication is comparatively less significant according to the Standards than expected, with ISO 22301 Security & Resilience having the highest weighted percentage at 0.31%. When ranked according to coverage of "communication", the top six Standards were Resilience Standards: ISO 22301, ISO 22380, ISO 22331, ISO 22384, ISO 22317 & ASIS SPC.1 Organizational Resilience. This strongly suggests that communication is more integrally considered when articulating the requirement for organizational resilience as a broader risk concern.

The analysis revealed that communication appeared most frequently adjacent to consulting, detailing throughout all documents the importance of this function at the various stages. However, noting this, only the OCEG Red Book highlighted the necessity to define communication methods, and the NIST 800-30 suggested vehicles for risk communication as an integral part of the risk assessment process.

STRUCTURAL ANALYSIS OF RISK MANAGEMENT MODELS

The structural analysis sought to identify structural consistencies and discrepancies between the various risk management models, with a number of structural observations:

- Of the 27 Standards reviewed, 12 drew on the risk management stages detailed in ISO 31000 – of these Standards, seven specifically referred to the risk assessment process detailed in the ISO 31000 (or its predecessor AS 4360) model.
- Structurally, 15 of the 26 models adopted a flow chart approach in their guidance towards achieving managed risk.
- Thematically consistent within these Standards is the presence of factors; establishing the internal and external context, identifying, analysing, and evaluating the risks, the provision of risk treatment, etc. with monitoring and reviewing, and communicating and consulting being integrated into all stages mentioned above.
- The identification of the decision maker is not explicit in many of the models and when mentioned, being within the "Establish the Context".

Identifying and connecting with the decision maker is not as prevalent as it should be

Given the importance of the decision maker within the process, further investigation was undertaken. When considering the decision maker, guidelines such as OCTAVE (Alberts & Carnegie-Mellon University Software Engineering Institute, 1999) and the ESRM model (Allen et al., 2017) indicated that the key factors considered by senior management was their perception of what constituted a critical asset or "what would they most want to protect" (Alberts & Carnegie-Mellon University Software Engineering Institute, 1999, p. 11). The analysis showed that "Top Management" was included in the ISO 22317 (2021) model; however, the emphasis was to communicate top priorities, and then approve results rather than in a decision-making capacity. Nevertheless, analysis showed that the detail behind these factors does little to explicitly encourage the risk assessor to identify the decision maker and align their message with their criteria and what they believe is critical.

Within the primary security risk management Standards reviewed, only the Homeland Security model referenced the decision-making stage specifically through their "Decide and Implement" stage, with a number of the other Standards implying a decision-making process. For example, the ASIS model has a YES/NO decision fork after the "Treat Risk" stage but with no articulation of what this process involves. Furthermore, across all reviewed models was the existence of the risk treatment stage occurring after the risk evaluation stage, yet only six of the Standards referring or alluding to the decision maker in this process. Of those six, only the most recent NIST guidelines, published in 2022, made specific reference to identifying the decision maker in the "authorise" step. This lack of general consideration of the importance of identifying the decision maker is also seen in the general Risk Management Standards; of those reviewed, only the OCEG acknowledged and was explicit in the requirement to align the presentation of the risk message with the criteria of the decision maker.

Findings demonstrated that most of the Standards showed a structure that led directly to the implementation of the risk treatment stage, without explicit engagement with the decision maker. Within all reviewed Standards there exists a feedback loop, in the existence of the *communicate* and *consult* and the *monitor* and *review* elements of the process encircling the entire process model. However, there is no reference to the requirement to communicate or consult with a defined decision maker, suggesting that the decision maker is the process owner. This is reflective of the word frequency count which

considered an external decision maker and a vital communication process, but with limited explicit need to identify these elements.

Flowchart vs. Cyclic Models

Eleven of the Standards reviewed adopted the process model of ISO 31000, where all models represented a top-down flowchart process that implied that each stage is completed before moving to the next. Many of these top-down processes had mentions of communication and consulting but with limited reference to refer to the decision makers until the end of the entire process. However, nine of the models reviewed presented a cyclic format highlighting the need for the process to be iterative and continual. Such an approach has been adopted by the ASIS ESRM guidelines, defining ESRM as an "an ongoing life cycle" (p. 70) and comparing it to a similar life cycle within the 2022 BCM Standard ISO 22331, DHS Risk Management Framework, US GAO Enterprise Risk Management Framework and the NIST Guidelines and Framework. Similarly, the latest iteration of AS 4811 included references to the cyclic approach through its model – an element missing from the 2006 version. It is observed that the ISO 31000 (and its derivative Standards) flowchart process has an iterative approach towards the monitoring and reviewing stage of the process only.

However, the only cyclic model that suggested an external decision maker is ISO 22301, which included the requirement for an oversight committee and to perform management reviews within this cyclic process. The cyclic model presented by ISO 22384 placed the validation stage after the treatment selection stage, again implying the decision maker is the process owner, with the external stakeholders only performing a compliance centric, governance role. Allen et al. (2017) accepted that these cyclic approaches did not prioritise the engagement of business stakeholders within the risk management process – a key component of the notion of ESRM. However, notably lacking from the discourse on the ESRM life cycle is the explicitness to identify the decision-making criteria and align the risk communication message to that defined criterion.

Nevertheless, a cyclical approach with key intersection points directly targeting senior organizational decision makers did emerge in the review of literature. This approach is highlighted in the works of Malone (2015) which acknowledges the strength of the Intelligence Cycle (Figure 4) in focussing towards directly informing decision makers stating "the important consideration here is that collection efforts must be driven by specific needs and requirements established by the end user". Malone (2015), highlighting through "Direction Needs, Requirements".

In contrast to the Intelligence cycle, the existing SRM Standards all take the approach and the assumption that the decision maker is the entity completing the risk assessment and that upon completion of the assessment, the next step is treatment identification and implementation. By contrast, the strength of the Intelligence cycle is the direction that the assessor must communicate their message back to the decision maker before receiving further direction, such as the treatment to be identified, evaluated, decisions made, and then projects implemented. The

Figure 4: **The Intelligence Cycle**

Source: Malone, 2015, P 54

intelligence cycle assumes the external decision maker directs every stage of the process.

This cyclical approach focussed on the decision maker being hierarchically outside of, and above the security position, is supported by Mintzberg (1979) and the notion of security being seated in the technostructure. Therefore, security does not have senior decision-making authority in terms of the allocation of capital resources.

STANDARDS ANALYSIS FINDINGS

The analysis found significant structural and thematic barriers to influence through the application of SRM tools and models which:

- lack ease of identification and use.
- lack clarity around terminology and language.
- fail to emphasise the significance in identifying organizational decision makers.
- contain inconsistent identification, communication, and consultation practices with, and for the senior decision maker levels within the operating core of the organization.
- fail to establish the assessment and business impact communication strategy.
- entwines treatment with the process of risk identification, analysis, and evaluation, as opposed to recognising such analysis is a core process in and of itself; and
- infer the security function is the decision maker in the risk assessment process.

The analysis led to the development of several observational findings (Table 5).

Table 5: **Analysis of Indicative Findings**

The plethora of overlapping and dynamic SRM Standards and guidelines makes the process of sourcing the correct and most up-to-date best practice information and processes less accessible to the practitioner.
RM is a process of managerial control over the organization. The more specialized the discipline, the more managerial control through verification and auditing is required from hierarchically senior managers.
There is a lack of clarity of language and consensus with definitions of key elements within the RM Standards. Linguistic nuances are a source of confusion and create barriers in the consistent messaging of risk communication.
SRM forms an integral part of the wider organizational activity and risk management processes; however, it is only one part of the wider risk purview.
ESRM is a misnomer as in the business literature, security is a technical specialist activity sitting in the technostructure. Such a seating is external to the operating core and strategic apex to organizational structure.
RM and SRM Standards are used primarily as an identification tool; information gathering to enhance the decision-making process; however, they lack the granular detail, depth analysis and impact in identifying, analysing, evaluating, and communicating treatments. The development of a mitigation strategy, while a risk objective is a secondary task in the RM process.
SRM is an information gathering exercise designed to inform and support the decision-making process of the operating core or strategic apex.
The decision maker and the decision-making process is an integral part of risk assessment; however, the identification of the decision maker is not explicitly discussed and is merely alluded to in the Standards and guidelines as a part of the "establish the context" stage. This lack of clarity around the identification of the decision maker, and subsequently a deep comprehension of the analysis, communication and process required, is a significant limitation.

Table 5: **Analysis of Indicative Findings, *Continued***

The final decision maker regarding allocation of capital in response to security risk management is hierarchically above the SRM practitioner within the organization. There appears to be a financial glass ceiling for SRM to achieve their objectives.
Influence for SRM is consolidated or enhanced through the communication and consultation process.
Communication is central to the risk management process, the absence of the requirement to explicitly identify the organizational specific communication methods within the risk management process is a limitation.
Security needs an agreed risk communication framework that sits within the wider organizational context.
Security risk identification and analysis and communication is a separate process to the identification, analysis, and communication of risk treatment options.
SRM Standards are primarily focussed on the assessment process and information gathering stage and have lesser concern with the broader business context.
The secondary/specialist RM Standards show that the more specialized areas focus on complying to an externally imposed regulatory environment and therefore, a smaller organizational sphere of influence.
General risk management does not have a focussed concern for SRM on an organizational level.
The general risk manager sits in the organization's operating core and is more concerned with the objectives and performance of the broader organization.
The general risk manager has a wider organizational focus and thus larger sphere of organizational influence.
General and specialist risk models assume that the decision maker is the process owner, or the SRM professional, moving immediately from assessment and analysis to treatment stage with, in most models, no acknowledgement of the requirement to present options and gain approval from an external decision maker – a clear barrier and limitation.
The absence to explicitly identify the decision maker and aligned communication techniques within the risk management process is a limitation.
The flow chart format of the risk management process implies that the provision of treatment is the defined end of the risk assessment process. The iterative feedback loop in many models is not as clear as other alternative options, which is a limitation of the models.
Risk Management models should be tailored to the organizational process and decision-making practices – with specific instruction to identify decision makers and communication methodologies and techniques.
The security risk manager is not the capital decision maker in the SRM process.
The security risk manager does not have the influence or authority to make organizational capital risk-based decisions and accordingly allocate required resources.

RISK EXPERTS SECURITY INFLUENCE

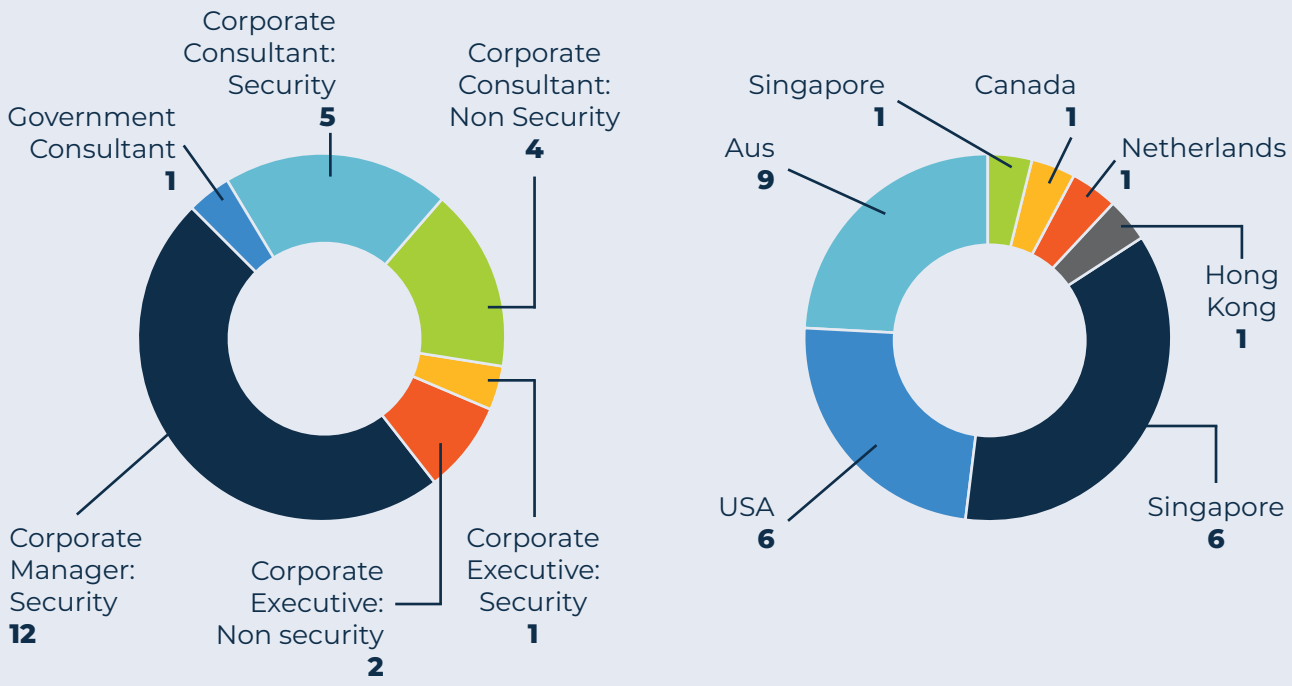
This stage undertook 11 focus groups, which included 25 business and security professionals, drawn from the business community and the ASIS International membership cadre ensuring a breadth of participants both in terms of job roles, hierarchical stratum positioning and nationalities (Figure 5). Central to the study was the ability to get a sample from across the organizational spectrum, allowing for all perspectives of SRM to be considered.

The focus group analysis crystallised many of the key challenges faced by security professionals in achieving the influence required to manage security risk. Many participants acknowledged the lack of understanding around risk influence in the corporate setting, with several stating there was significant need for continued conversations. For example, one participant stated that "this topic is one of the fundamental problems with security management and has been for a long time." The focus groups cemented overarching themes negatively impacting security professionals' ability to achieve robust risk influence. These themes included: organizational management, risk models and their authenticity, risk and business communication and other factors of influence such as perception, education, regulation, and leadership attributes.

ORGANIZATIONAL MANAGEMENT

Security professionals noted the existence of an organizational hierarchy that potentially reduced risk influence for security. However, a dichotomy

Figure 5: **Focus Group Participants by Location and by Joe Role**



emerged, between those who recognized security as a specialist area, sitting outside of the organization's core business, and those who saw security as being so imbedded with every facet that they were of the view such role division did not exist. Furthermore, security participants felt that as the role of a general risk manager (Chief Risk Officer, Chief Information Security Risk Officer, etc) is a recent organizational development, the management seating is still in its infancy and therefore hard to define as per the management texts. The focus groups specifically highlighted difficulties with defining the "security" role, differentiating between physical security and other forms (IT, network security, etc) with most participants placing physical security professionals in a different section of the organizational hierarchy to the IT security department. Many participants felt that influence is not necessarily derived from hierarchical ranking per se, but from other factors including an individual's personal traits.

A focus group Likert Survey provided perceptual ratings of corporate security risk influence, with participants reporting that they had a moderate to high level of risk influence (M4; SD 1.35), and a moderate to high level of communication effectiveness (M4; SD1.46). Of note, Corporate Security Managers ranked their influence as lower and their risk message less influential than corporate security executives.

However, the self-reported Likert ratings were shown not to be consistent to follow up discussion, with many security professionals reporting they had no influence across corporate decision-making despite their initial rankings. For instance, a participant who ranked his influence as an above average 5 later stated, "I have no authority at all…I have as much influence as my foot". Upon reflection, participants stated they would probably reconsider their initial perceptions and lower their influence ratings.

Furthermore, context emerged as a significant contributing factor to risk influence, with

Table 6: **Self-Reported Influence and Communications Effectiveness**

ROLE TITLE	INFLUENCE OF SECURITY RISK	EFFECTIVENESS OF SRM COMMUNICATION
Corporate Consultant – Non-Security	4	4
Corporate Security Consultant	3	3
Corporate Executive – Non – Security	3	2
Corporate Security Executive	5	6
Corporate Security Manager	4	5
Government Consultant	3	4

one participant stating a previously high level of working influence when working in critical infrastructure, with direct C-Suite access and influential networks. However, upon moving to a media organization his influence of security was considerably reduced, highlighting the relationship between organizational context and security risk influence.

Also emerging was a disconnect between how security saw their hierarchical position within the organization and how others across the broader organization see their level of management position. As one participant described:

> *We view ourselves as being something that the rest of the organization doesn't see when they look at us. In my career, in my dealings, I think that there are more security managers and executives that think they are higher up than they actually are across the board.*

Concurring, another participant stated:

> *Perhaps security influence doesn't exist…It's why you have a consultant because they don't listen to their internal people. So, they get the external person to come in and…say the same thing that the internal person was saying, but they'll listen to the external.*

A lack of influence view was supported when the participants self-assessed their hierarchical position in accordance with Jacque's organizational hierarchy framework (Jacques, 1989). These assessments found that half of the security managers ranked themselves higher in the hierarchical standings than the research assessment using a risk outlook measure (e.g. risk outlook of 5 years, 10 years etc), a finding consistent with the Ludbey's study (2018) into the security stratum of work and occupational ceilings.

RISK HIERARCHY AND CORPORATE INFLUENCE

All participants acknowledged that security was a crucial piece of the overall organizational risk puzzle; however, they felt that security risk is not salient for those concerned with wider organizational risk. Participants felt that security risk is often seated under other, more general business units such as safety or facilities, and therefore security risk forms a part of that larger business unit operational risk concern. Nevertheless, several participants believed no risk hierarchy existed within their organization, rather all risks were considered individually, depending upon context. However, upon deeper exploration this was consistently contradicted within the sphere of cyber risk, where participants expressed this area was given preferential treatment. This suggests that a risk hierarchy is present in all organizations, even if it is not formalized or fully understood. As several participants discussed:

> *Participant One: Within cyber, there is a healthy fear, and you know, you sell fear…*
>
> *Researcher: So, the fear of the unknown?*
>
> *Participant Two: One hundred percent. We can't control it, we don't understand it, throw money at it.*

When considering operational risks, participants believed that cyber risk would usually trump security for resource allocation. They expressed that cyber risk gets more influence than security in general because of fear of the unknown, immediacy, or reputational implications, which are not usually considered to be factors in physical security centric risk. In contrast, other corporate security activities were seen as manageable, well understood, controllable and low dread. This view is evidenced by one participant who stated:

Security Risk is the stuff that for the most part, we can insure against…we can insure against break-ins, we can insure against theft. What we can't insure against so easily is reputational damage…third party…supply chain…it's not so easy. If we are talking physical security, any business nowadays in 2022 should have the physical things already in place and it really is just a case of upgrading and updating.

Participants who saw cyber risk as being more important, believed this to be due to cyber event impacts having potential strategic consequences, whereas a security incident is rarely believed to have a strategic impact. This factor was a key point of discussion, with several participants advocating that security risk is often entwined with strategic risks, but this is poorly understood as evidenced earlier in the case study. Such a view highlighted an opportunity to ensure that security risk is better communicated in terms of

its strategic impact. The majority of Corporate Security Managers reported that after compliance, cyber was hierarchically more important. This led to an important point being raised by non-security Executives and Consultants (and those participants who had started in a security role but progressed to non-security/risk/executive roles), that this response highlights how siloed the security professional can be; stating that security managers are missing the bigger picture of enterprise risk across the entire organizational spectrum.

The themes which emerged included the view that security risk is treated as an operational risk rather than one of strategic significance. Furthermore, a risk hierarchy exists within organizations, and this is poorly understood or articulated, resulting in missed opportunities and further disconnect, ultimately leading to reduced security influence amongst organizational decision makers.

ENTERPRISE SECURITY RISK MANAGEMENT – AN ORGANIZATIONAL MISNOMER?

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 are 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 1! … 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 (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 ESRM provided both mixed, and sobering results. For instance, three participants – all of whom were Corporate Consultants, Non-Security – pivoted this discussion to suggest the 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 as to the role and importance of the security function, indeed if it had a role at all or was merely "one tool in the risk mitigation toolbox".

One Corporate Executive (Non-Security) provided examples of an organizational risk taxonomy, il-

lustrating 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 programme or an organizational Risk Taxonomy, the significant majority of participants from non-critical 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.

One security manager highlighted that he was aware of an enterprise level risk taxonomy but "that's way above my level" highlighting again the hierarchy and relegation of security risk to the lower echelons, and indeed being omitted from the broader organizational risk conversation. This supported the premise that notwithstanding best intentions to understand the organizational context, one of the biggest limitations to attaining influence by security professionals is in understanding the broader organizational risk context and being able to leverage that information successfully. As one security manager stated:

> *We get this instruction to "establish the context" – blah blah, and we go and do our facility characterisation and we ask about their risk appetite because that's what we think risk context is, but the fact is, we have absolutely no idea about the risk context of our business. I know that money .. for new CCTV is going on SOCs and networking and whatever, but I don't see anything else because I'm not part of those conversations and unless I've been through the ranks, I don't know what I'm asking. You talk about a taxonomy? I bet most security managers have no idea what that is.*

RISK MANAGEMENT MODELS & THEIR AUTHENTICITY

Focus groups highlighted that formal risk standards were not as widely used or considered as expected. Many participants questioned their authenticity, or the usefulness of various risk models and frameworks available, but when asked, they listed multiple sources of frameworks and Standards. Of interest was that seven of the 25 participants interviewed (USA (3), UK (2) Aus. (1), Canada (1)) used either no Standard or no specific Standards; four of these participants said this was because they use client or organization specific processes that do not specifically align to a given Standard. The remaining three participants stated that in their experience, the processes used are an amalgamation of various Standards (ISO 31000, ISO 27001, ANSI ASIS RIMS Risk Assessment) and they could not align to a specific model.

Nevertheless, participants expressed that the plethora of published risk standards was a benefit to practitioners, allowing choice of relevant elements depending upon the organizational context and risk assessment needs. Numerous participants went further, asserting that reducing Standards and trying to silo security risk practice further would be counter-productive and would reduce Security to "the level of a barista or real estate agent where they do a three-day course supplemented by a Standard". However, of those participants stating that the variety is a benefit, it was felt by several that there are also drawbacks that require active consideration, as highlighted by one participant:

> *All professionals have toolboxes, you don't build a house with a screw-*

driver. You have multiple tools and resources to use. I think that equally the fierce competition that has evolved between the UK and the US in particular in the last several years between who has the most superior Standard, I think is elevated the pursuit of it, but not necessarily consolidated. The… NIST seems to have a printing press of Standards at the moment for every sort of thought process and threat vector and problem. They're advancing. But I think it's also contributing to the noise and the problems. And even being a professional it's difficult to keep up with so many of them are being minted on a regular basis.

However, other participants supported the view that too many standards existed adding to the complexity, and providing a barrier to influence, stating, "security professionals are "bombarded" by the "noise", even calling it "white noise" that is "overwhelming". These participants believed this specifically creates "a huge challenge for smaller organizations" suggesting it was part of the complications of the job role in keeping up to date with the latest Standards. It was discussed that larger organizations had the resource to purchase and keep abreast of the changing landscape, however smaller organizations often opted out of managing the changing and varied Standards, preferring to employ external consultants, or in some cases, ignoring the updates and changes altogether, using it as an excuse to not address security risk.

The notion of consistent application of Standards was considered by the groups to be extremely mixed, with participants reporting that in critical infrastructure and government environments, Standards are generally applied consistently and effectively. However, in the private sector and non-regulated industry, this was not the case.

According to participants, application was oftentimes piecemeal and inconsistent, often treated as a tick box activity, a view espoused by one participant, "I think for a lot of companies, it's just to demonstrate they have a risk management response for optics purposes." Managerial control was also discussed in the context of security risk management compliance, with many participants feeling that there was only a tangible managerial control within those critical infrastructure or highly regulated industries or those where the accreditation is auditable. Participants found this to be a significant limitation, and the influence of security is lessened because adherence to Standards. For example, they felt that ISO 31000 is non-auditable and often an exercise in paying lip-service, a view reinforced by one participant, "I think for a lot of companies, it's just to demonstrate they have a risk management response for optics purposes."

Furthermore, participants identified the inconsistent application of Standards as being directly linked to the decision by their clients or organizational decision makers to use their own internal version of a risk management process rather than formally published documents. When questioned on who chooses this process, or where this process originates, responses suggested it was dictated by higher decision makers who either didn't trust the security role to integrate, or who were happy with whatever existing framework they were able to find themselves. As one participant stated:

I feel like I'm banging my head against a brick wall…From what I can tell, it has been in the company for years and years…and there's never really been an incident or a problem… so it's never been changed. It is not something I'm happy with, I have attempted to change, improve, circumvent, but I've been told, if it's not broken, why am I trying to fix it?

MODEL FORMAT

Participants generally acknowledged that front-line security practitioners and managers were not familiar enough with the technical aspects of the Standards, limiting their ability to comment on the limitations of the format itself. However, all participants consistently agreed the key to success and ultimately influence in security risk management lay in the assessor's ability to effectively establish the context and communicate the security message within that context rather than focussing on the specific tools. This point was well supported by those more senior participants who were more acquainted with models and had worked in the development of Standards, frameworks and processes. Consequently, it was found that the accuracy in establishing the risk context was more of importance for achieving security risk influence rather than any specific model or format. As one participant stated:

> *Every business has context; every business needs to be protected. Really, if we don't understand that bit, the rest of the process is a waste of time. And this is where the whole thing lies, is that security needs to understand it's context; it's not about being the corporate policeman anymore, it's about protecting the ability of the organization to continue... and we find out what that looks like by establishing the context.*

All participants supported the view that establishing the context was often poorly done, with security rarely fully understanding their full organizational context, including their organizational risk context. This results in failure to understand the business needs, a lack of understanding of where security fits in to the organizational framework and a communication disconnect in terms of treatment.

This finding highlights the implied understanding, yet lack of explicit direction towards a risk context. As one participant commented, "If anyone is out there who says they can give you a risk template, they're lying to you...they can share concepts and ideas, but ... no one can share a template because they all see and interact with risk differently."

THE CORPORATE DECISION MAKER AND SECURITY RISK MANAGEMENT

Security professionals are not the corporate decision makers – highlighted by a participant who stated: "I like to talk about risk management in the context of this as the process we're using to support your decision-making. The decision maker is never security." Participants noted that the decision maker for security risk management was often a senior executive, non-security; for most participants, security risk decision-making fell under the auspices of Health and Safety, Facilities Management or Operations. That is, organizational managers above or outside of the security function. Furthermore, it was found that in smaller companies the decision maker was often the Head of Finance. In the more risk-mature or compliance-based organizations, a Chief Risk Officer or similar was the ultimate decision maker for security risk decisions.

However, participants in compliance driven (e.g., financial services, banking) or critical infrastructure environments (airports, nuclear energy plants) reported a degree of decision-making influence in terms of resource allocation, but still reporting more senior approval required over certain levels, often building assumed rejections and resubmissions into the plan. Many participants believed that the security risk management process is an information gathering process, with two particpants – both corporate managers – security – clearly stating that in their roles, it is "just" an information gathering exercise for the decision maker.

It was expressed that Standards do not effectively specify that the decision maker is outside the SRM process, or the requirement for security managers to engage with them at the establish the context stage. Whilst they may acknowledge within the detail that the decision maker needs to be identified to allow contextually appropriate communication, it is not explicit within any of the models used, with very limited exceptions. The model formatting was discussed, and it was concluded that there is an incorrect assumption that the decision-making process is part of the role of the risk assessment process owner, or the security manager, which it is not.

RISK IDENTIFICATION OR RISK TREATMENT?

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 felt that essentially, security risk assessments are often being prepared and presented based on the judgement of the risk process owner as to the company risk tolerance, appetite, and budget, which more often than not, is not "in their wheelhouse", that is, outside their context or authority.

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 then 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 identified earlier. 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. For example, upon identifying risks a security manager may use a Business Impact Analysis which allows the decision maker to see the impact of the risk. The decision maker decides if it is acceptable or not and the security manager would then prepare a Cost Benefit Analysis, comparing various treatment options, perhaps presenting an ALARP framework.

RISK AND BUSINESS COMMUNICATION

Communication of the risk message was found to be a salient theme, specifically, influence is significantly enhanced through clearer communication, and that communication is a current key weakness, but could be a strength if done well. Participants all agreed that "security must speak the language of the decision maker".

Who is security communicating to?

The ability to communicate directly to the requirements of the decision maker using the correct language and tools, was identified as 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 felt in current models the instruction to communicate and consult with the decision maker at all points of the process was too broad and lacked meaningful guidance on how to communicate influentially.

Why is security communicating a risk message?
Translating the operational risk from a security threat assessment into a comparable risk language that is understood and accessible by the senior decision makers was reported to be 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 won't understand.*

It was considered a necessity for security managers and executives to understand and communicate the breadth of purview across the organization they are observing and assessing, to demonstrate that security risk is not actually siloed but has broader, systems focused outlook. This view was important to demonstrate links to strategic level impacts. Whilst many of the participants recommended highlighting the impact and consequence factors across the entire organization, and making security a "force-multiplier", it was generally agreed that usually 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 it was acknowledged by many in the groups that 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 of, oh my... But often security threats unless it's .. visceral or exciting, like terrorism or cyber breach, people can't relate. It's too abstract. And so therefore, how 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 than just - we have a policy, well, you know what, it depends on the context and how that was understood.*

Many viewed this being as a result of the various operational backgrounds – typically military or police, with less emphasis on formal business studies and skills. The recruitment of security managers from these industries was seen by participants as a double-edged sword. As one corporate executive stated "it is nice to have existing clearances [from police or military background] because that saves me money, but being a brilliant operator doesn't always translate into a business environment... I must teach them Corporate." Participants noted that the benefits of hiring pre-vetted and operationally focussed military or police often meant sacrificing the business knowledge required for that level, with those indivisuals often lacking in the ability to translate an operational risk into a strategic business concern.

What should security management be communicating?
The importance of communicating indicative

business impacts and consequences aligned to security threats was the salient issue according to participants. More specifically, the impacts as they are directly aligned to the business objectives, where such direct communication would enhance influence within an organization. It was subsequently also acknowledged that the nature of the security function often meant that doing the job successfully, meant there was nothing to report. Consequently, security also needs to clearly communicate how it is being effective to mitigate indicative risk.

CLARITY OF LANGUAGE

Most participants considered that the lack of linguistic clarity of numerous terms caused considerable confusion in achieving security risk influence. As one participated 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 cyber security.

- Several linguistic concerns were raised by participants which they believed had an 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, which as terms are often used interchangeably and incorrectly as synonymous were also identified as a barrier to effective security risk influence. Participants suggested that misunderstanding of these key concepts often happened at 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 standardisation is key to achieving better risk message influence, not only within an ERM framework but also directly aligned with the analytical metrics being used. Such alignment would enable more effective comparison of cross-organizational risk typologies. Participants felt to achieve this level of organizational embeddedness requires both higher level, and broader general risk management training, often not available to or taken up by security managers. Again, the theme of broader management education for security managers was evident.

FACTORS OF INFLUENCE

Participants generally rejected the idea that influence is derived from organizational positioning, discussing instead the following as factors of influence:

- Perception of Security and Corporate Attitude to Security Risk Assessment

- Professionalisation

- Regulation

- Leadership Attributes

All participants agreed that the security manager generally lacks influence. As one participant opined: "All these Standards take the viewpoint that the senior security official or executive within the organization, is operating at a level that has direct influence on the C suite. And I do not believe that that's the case at all."

PERCEPTION OF SECURITY & CORPORATE ATTITUDE TO SECURITY RISK ASSESSMENT

Perception of security played a salient role in the influence given to the function and participants agreed that security is subject to several negative connotations. Most participants, including those from the regulatory risk-mature industries acknowledged that the inherited stereotypes of security continue to be a significant hurdle in security achieving stronger organizational influence. Participants discussed the security function as being seen as the "corporate police", "naysayers", "doomsayers", "...just guards, gates, and guns", "a paramilitary role" and "dark figures", amongst others.

Furthermore, it was highlighted that in the C-Suite, the security function is rarely seen or heard from unless there has been a significant incident that has a strategic implication or loss. The negative connotation was also frequently paired with the notion that security is perceived as providing little value; being dubbed "a drain to the bottom line", where "security always comes at a cost...it never actually gives you anything". This narrative linked the negative connotations of the security function to the fact that if physical security is being "done correctly" then it is invisible and the visible elements such as the guards on gates, typically control areas, reduce access and limit freedoms. Corporate Security Managers were of the view that the negative perception of security is the most significant issue, as one manager stated "I genuinely think the optics of the role is the biggest hurdle we've got."

However, the response to this was stratified; the Organizational Executives, both security and non-security considered that indeed this was a limitation to achieving sound influence but noted there were many more significant limiters. Participants did acknowledge that this attitude is regularly being challenged with security professionals striving to show added-value through being a "force-multiplier" within different organizational functions. For instance, several of the participants acknowledged that their organizations were actively embracing a risk-based approach to organizational management, in particular security was falling under the risk management portfolio, and that resulted in the increasing awareness and influence of security risk.

Noting the growing move towards accepting the importance of security risk, several participants noted the reality within an organization is often different. Many business functions were often unwilling to work with the security function due to its siloed nature, where the perception of security as "someone coming into my department to rat me out". What became clear through discussions is that often, the perception of security inhibited the integration of the function within the organization, suggesting that even awareness of the organizational context may sometimes not be sufficient when attempting to integrate. The importance of understanding of the roles of all other business functions, and of those business functions understanding the security function, is key to leveraging the knowledge gained by establishing the context at the start of the risk management process.

The perception of risk from security managers was also highlighted as a limitation. It was noted that often due to a tangible lack of understanding of risk beyond the matrices used, security managers incorrectly dub themselves to be security risk professionals as opposed to security managers with an understanding of security risk. It was suggested by non-security Executives

that security professionals using the title "security risk professional" would be met with derision amongst their specific risk management qualified peers. Whilst this view was not consistent across all, these views were held by participants in the Executive and non-security roles, uncovering a significant negative perception of the security function from more senior managers. Such views supported the discourse identifying the security risk assessment process being treated as a tick-box exercise, following a template, and being disconnected from the broader organizational risk context. This issue was discussed by one participant, stating:

> *The security perception of risk is just using a template that identifies impact and likelihood and using that to justify whether to have one guard or two. Security is no more risk focussed or linked than the layman doing an HSE assessment for a school sports day. Security should be a specialist risk type, under a broader Operational Risk framework.*

The poor understanding of the corporate security function at the Board level was also raised as a barrier. A disconnect emerged between the perception of the security managers and the executive or non-security; with the corporate security managers often expressing that the C-Suite/Board/decision maker does not value security risk because it does not fully understand it or its importance (for example, the concept of security decay theory). Conversely, when discussed at executive and external consultant level, the response centred on there being no need for the Board to understand security in this way – this was the role of the specialist – with the crucial requirement being not the ability to translate specialist security knowledge for the Board to understand, but the ability to communicate the security risk in business organizational risk terms and language for the Board to be able to compare and utilise. Participants agreed that the managerial skill of understanding risk context and communicating accordingly is a key factor in attaining influence. As one participant explained:

> *Security remains an abstract, solutions-centric construct within most organizations. That is, someone has already determined the risk, which has a 'security' relationship, so a person or department is prescribed to manage it. Hence, security is the risk management solution, not diagnostic or assessment discipline. Following on from this, 'security' is an abstract concept, related to providers, people, technology and known services. Security fences, locks, guards, mobile patrols, and security activity all fall under this banner. As a result, security needs to be represented and considered further upstream in the risk discourse of the C-Suite, strategic risk(s), climate risk, operational/enterprise risk, etc. However, this requires broader, more specific skills and qualifications of practitioners.*

RESPECT & PROFESSIONALISATION

Professional disrespect was also highlighted during the discourse as a significant barrier to risk influence. It emerged that often the role of the security professional is seen with a degree of disrespect, and despite the accepted growing awareness of Risk, participants found that often the role of security was "discounted" in discussions of risk at Board level, with participants attributing this lack of respect to numerous factors. These factors included the perceived misuse of the term "security risk professional", and the traditional trajectory into security, with many security managers emerging from a military or police background with significant operational, but

very limited corporate or business experience. Embedded in this view was that the Board often perceived the security professional as educationally inferior to other organizational professionals, such as lawyers or accountants, who have sound vocational degree qualifications.

Similarly, participants found the lack of risk maturity across industry a contributing factor with operational/physical security professionals not holding as much gravitas amongst the hierarchy as their peers – this was noted, with cyber and network security experts who often must be degree qualified. As one participant stated:

> *If you look at the chief security officer and chief risk officer, the Protective Security Policy Framework generated a whole new generation of chief security officers. One morning some people woke up with a post it note on the desk saying you're the new CSRO. That was because they had to have one. And the chief risk officer materialized much the same way in a lot of banks and other organizations. If you look at the lineage of their careers, at some point, someone went from being a barista, a real estate agent, an Uber driver to being a security manager or risk manager - and I'm being very disparaging with that - but nine times out of 10, transitioning from some other role into that title. There now there's the security manager or the risk manager and that's not necessarily how every other profession works. You don't go from property manager to orthopaedic surgeon but it happens in security risk all the time.*

EDUCATION

Professionalisation of the industry through education was consistently brought up when discussing both limitations and opportunities to influence. Several of the participants had completed tertiary degree qualifications in Security and/or Risk and were able to articulate the tangible differences having gained these, both in terms of transferable skills but also in terms of perception and ultimately influence. Furthermore, participants felt it was important to distinguish between professional certifications and more formal tertiary degrees, stating that some of the current security certifications, "relegate security to the level of baristas and real estate agents; a three-day course supplemented by a Standard."

Participants consistently formed the view that the future for enhanced security influence was seated within the notion of the "Pracademic"- having the operational experience but the academic tertiary qualifications, including the wider academic theoretical knowledge to underpin it. Examples given including theoretical knowledge across psychometric dread risk, security decay, and business skills such as communication and leadership training (MBA and C-Suite language). Participants felt that the focus by various standards was upon the process itself; where it was noted that there was very little, if any, coverage of academic background theories, focussing instead on the prescriptive following of a flow chart process. Furthermore, participants found that professional development content often focussed again on the security processes rather than the academic understanding or business education. This discourse suggests that security risk training and qualification content requires academic broadening to include subjective human elements currently seemingly reserved to more formal academic study. All participants considered that better academic and business-educated security managers can engender stronger influence. As one participant illustrated:

> *Why do you need a degree in security, because most people think of the*

guy standing in front of the pharmacy, the security guard sitting there behind a camera screen … That's not what I do. To be a successful and effective security manager, I have to understand some seriously complex social theories, the built environment, threat, vulnerability, intelligence, I need to understand physics, even maths, I need some psychology, I need business speak. Being a police officer for 15 years didn't prepare me for that. I go into meetings now and I know the theory behind the guns and the guards and the gates. I know my stuff and that makes a difference in being heard.

REGULATION

Participants felt that those security managers who were seated within a highly regulated industry, or sector had a better chance of achieving risk influence than those outside of such an environment. This aspect includes those industries considered to be critical infrastructure or those heavily regulated industries. However, it was also noted that such influence depended on where in the organizational structure the security department reported to; with those who reported to departments with a compliance or regulatory obligation such as Health and Safety, typically being treated as having "more nitty gritty influence than if they sit under facilities". One participant argued, "…if security had the same regulatory stickiness that health and safety has, we wouldn't be having this conversation."

Leadership attributes

It was found that security's sphere of risk influence was a factor of an individual's personal attributes, rather than something tied to the corporate security sector function. The initial analysis of the Standards found limited evidence of personal and managerial attributes; however, the individual leadership qualities – rather than managerial skills – featured heavily in the focus group discourse.

It was considered that the security function lacks deeper respect and is narrowed and siloed. However, individual security professionals achieve the necessary degree of risk influence through their personal attributes which included: charisma, personability, empathy, foresight, business communication ability, education and deep understanding of security body of knowledge and theory, personal connections and network, flexibility, and the ability to make and leverage C-Suite relationships. As one participant stated, "influence is achieved through personal networks… through constant tests and adjustments…through representing the problem to the people and speaking to the right ones, it's about gaining their trust, and with a degree of panache along the way."

PROJECT FINDINGS

Through a review of literature, and analysis of the security risk management and risk management Standards, and 11 subsequent expert focus group discussions, the project was able to uncover significant limitations to, and opportunities for enhancement of the influence of security risk (Table 7).

The perceived corporate influence exerted by the SRM professional

The corporate-organizational function of security is still laboring under inherited image issues – that of the naysayer, the corporate policeman and the drain to the bottom line. There are still significant negative connotations associated with the security function resulting in a lower level of influence. This aspect was reinforced through a perceived degree of professional disrespect for security, acknowledging that many security professionals learn their business through policing or military careers, as opposed to attending University where standardized educational programs impart foundational business knowledge with degrees of prestige. Consequently, despite the best efforts of the industry to show added value and the strategic implications of their operational risk portfolio, security at best is still considered an operational risk, seated on the bottom of the risk hierarchy; and at worst, "just" a risk treatment strategy rather than a meaningful business activity and risk typology in and of itself. Finally, it was expressed that the lack of auditable regulation within the industry has relegated security to a systems maintenance role rather than a vital compliance adherence factor, reinforcing the negative perception of security. The result, ESRM is not achievable noting the current barriers to security risk influence.

How security risk management can more effectively influence corporate decision-making

The study found that security risk models, and their usage require adjustments to meet the structural and stratum seating of corporate-organizational security. Current risk models were considered inauthentic, incorrectly assuming that the process decision maker is the security manager. This creates a time and place consultation issue within the risk assessment processes, as to when the decision maker is consulted, with most models bringing the decision maker in explicitly at the point of treatment implementation, if at all. This cauterizes the process; with security managers selecting analysis techniques and treatment options based on specific identification analysis techniques such as business impact analysis and according to the organizational risk appetite. Consequently, beyond the remit of the security function due to factors such as their hierarchical seating and their lack of awareness of broader organizational activities and risk context.

It was considered that security can increase its sphere of risk influence by leveraging and utilizing their individual personality, charisma and leadership attributes to overcome the negative connotations of corporate security. This includes building personal and professional respect through their networks. In addition, prior to undertaking risk assessments security managers and executives should directly engagement with key general manager decision makers, to allow deeper understanding of requirements in terms of language and analysis tools used, organizational and personal priorities (including psychological dread factor). Active engagement with an organizational ERM program where present and seek to understand the formalized or informal risk hierarchy or taxonomy. This would enable appropriate relationships to better leverage their position as a force multiplier and to ensure that their work is aligned with the organizational risk goals based on the C-Suites' perspective across

the entire organization, rather than the security perspective, looking upwards. Finally, the use of more quantitatively evidence (e.g. cost benefit analysis, contemporary case studies) would added value to the risk messaging, highlighting the operational and strategic impacts of any operational security risks using translatable tools to ensure that risk messages are communicated in a manner to enable direct business comparisons with other risk typologies across the organization.

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.

REFERENCES

Abbott, A. (1988). *The system of professions : an essay on the division of expert labor.* Chicago: University of Chicago Press.

Alberts, C., & Carnegie-Mellon University Software Engineering Institute. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* United States: Carnegie-Mellon University Software Engineering Institute,.

Allen, B., Loyear, R., & Noakes-Fry, K. (Eds.). (2017). *Enterprise Security Risk Management : Concepts and Applilcations.* Brooksfield: Rothstein Associates, Incorporated.

ASIS International. (2015). ASIS International Risk Assessment Standard. In. Alexandria, VA: ASIS International.

Borodzicz, E. (2005). *Risk, crisis and security management* [1 online resource (xi, 244 pages) : illustrations]. Retrieved from http://www.123library.org/book_details/?id=7269

Briggs, R., & Edwards, C. (2006). *Business of Resilience : Corporate Security for the 21st Century:* Demos.

Brooks, D., & Corkhill, J. (2014). *Corporate Security and the Stratum of Security Management.* London: Palgrave Macmillan.

Chase, R. (2014). *Security leader insights for risk management : lessons and strategies from leading security professionals.* doi: https://doi.org/10.1016/C2013-0-15989-2

Coole, M., & Brooks, D. (2021). Physical Security: Best practices. In L. R. Shapiro & M. Maras (Eds.), *Encyclopedia of Security and Emergency Management.* Perth, Western Australia: Springer International Publishing AG.

Dionne, G. (2013). Risk Management: History, Definition and Critique. *Risk Management and Insurance Review, 16,* 147-166.

Fayol, H. (1930). *Industrial and General Administration* (J. A. Coubrough, Trans.). London: Sir Isaac Pitman & Sons.

Hopkin, P., & Institute of Risk Management. (2014). *Fundamentals of Risk Management : Understanding, Evaluating and Implementing Effective Risk Management* [1 online resource (448 pages)](3rd ed. ed.).

Jacques, E. (1989). *Requisite organization: the CEO's guide to creative structure and leadership.* [Arlington, Va.]: Cason Hall.

Jacques, E. (1996). *Requisite Organization: A Total System for Effective Managerial Organization and Managerial Leadership for the 21st Century* (2nd ed.). Arlington, VA: Carlson Hall and Co Publishers.

Juliusson, E., Karlsson, N., & Gärling, T. (2005). Weighing the past and the future in decision making. *European Journal of Cognitive Psychology,* 17(4), 561-575.

Kinsey, M., Gwynne, S., Kuligowski, E., & Kinateder, M. (2018). *Cognitive Biases within Decision Making during Fire Evacuations Fire Technology* (March, 2018). doi:10.1007/s10694-018-0708-0

Kleiner, A. (2001). Elliott Jacques Levels With You. *Strategy & Business,* 22.

Lefler, R. (Ed.) (2015). *Chapter 10 - Is Enterprise Risk Management (ERM) Leaving Security Behind?* Boston: Elsevier.

Ludbey, C. (2018). *The Corporate Security Stratum of Work: Occupational Ceilings, Progression, and Career Success.* Edith Cowan University,

Ludbey, C., Brooks, D., & Coole, M. (2018). Corporate Security: Identifying and Understanding the Levels of Security Work in an Organization. *Asian Criminology,* 13, 109-128. doi: doi-org.ezproxy.ecu.edu.au/10.1007/s11417-017-9261-x

Malone, R. (2015). Protective intelligence: Applying the intelligence cycle model to threat assessment. *Journal of Threat Assessment and Management,* 2(1), 53-62. doi:10.1037/tam0000034

Martin, J., & Fellenz, M. (2010). *Organizational behaviour & management* (4th ed.). Hampshire: Cengage Learning EMEA.

Mintzberg, H. (1979). *The structuring of organizations: a synthesis of the research.* Englewood Cliffs, N.J.: Prentice-Hall.

Mintzberg, H. (1980). *The nature of managerial work.* Englewood Cliffs, N.J.: Prentice-Hall.

Mintzberg, H. (1983). *Power in and around organizations.* Englewood Cliffs, N.J.: Prentice-Hall.

National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments, Special Publication 800-30,. In *Information Security.* Gaithersburg, US.,: US Department of Commerce, Computer Security Division,.

Pettinger, R. (2010). *Organizational Behaviour : Performance Management in Practice.* London, UNITED KINGDOM: Taylor & Francis Group.

Poppe, S. (2016). What Exactly Is a Risk Decision? Retrieved from https://www.fairinstitute.org/blog/what-exactly-is-a-risk-decision

Sennewald, C. (2011). *Effective Security Management* [1 online resource](5th ed.). Retrieved from http://www.books24x7.com/marc.asp?bookid=41851

Simons, R. (2005). Designing High-Performance Jobs. *Harvard Business Review, July-August 2005* (July-August 2005).

Standards Australia. (2006). HB167:2006 Security Risk Management. In. Sydney, Australia: Standards Australia.

Standards Australia. (2022). Standards Australia - What is a Standard? Retrieved from https://www.standards.org.au/standards-development/what-is-standard

Statoil. (2013). *The Attack on In Amenas.* Retrieved from https://www.equinor.com/news/archive/2013/09/12/12SepInAmenasreport

Strategy Unit. (2002). *Improving Government's Capability to Handle Risk and Uncertainty.* London, UK Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ http://www.integra.com.bo/articulos/RISK%20IMPROVING%20GOVERMENT.pdf

Sum, R. (2015). Risk management decision-making: the analytic hierarchy process approach. *Journal for International Business and Entrepreneurship Development,* 8(2), 108. doi:10.1504/JIBED.2015.070442

The Cambridge Dictionary. (Ed.) (2022) The Cambridge Dictionary. Cambridge, UK: Cambridge University Press.

Wong, C. (2018). Bridging Worlds. *Security Management,* 62(7), 38.

Wren, Bedeian, A., & Breeze, J. (2002). The foundations of Henri Fayol's administrative theory. *Management Decision,* 40(9), 906-918.

Zhu, T., Haugen, S., & Liu, Y. (2021). Risk information in decision-making: definitions, requirements and various functions. *Journal of Loss Prevention in the Process Industries,* 72. doi:10.1016/j.jlp.2021.104572

ABOUT THE RESEARCHERS

DR MICHAEL COOLE

Michael is a Senior Lecturer and researcher at Edith Cowan University. He has 25 years of experience in the security, crime prevention and emergency management fields, and has worked in the Australian Defence Force, Western Australia's Department of Justice and as a private consultant. Michael researches and teaches across the broad spectrum of security and crime prevention problem domains.

NICOLA LOCKHART

Nicola lectures and researches risk at Edith Cowan University where she is a PhD candidate. With a background in Law, she has over 15 years of experience as a security and facilities professional and has provided security management and consultancy services to high risk government agencies in the UK and Europe.

JENNIFER MEDBURY

Jennifer lectures and researches in intelligence and terrorism studies at Edith Cowan University. She has over 11 years of experience as an intelligence analyst and senior intelligence analyst with the Australian Defence Intelligence Organisation and the Western Australia Police Force.