2019

The corporate security stratum of work: Occupational ceilings, progression, and career success

Codee Roy Ludbey
Edith Cowan University

Edith Cowan University

Copyright Warning

The corporate security stratum of work: Occupational ceilings, progression, and career success

A thesis submitted in partial fulfilment of the requirements for the award of:

Master of Science (Interdisciplinary)

Codee Roy Ludbey

Edith Cowan University

School of Science

2019

ABSTRACT

To meet the challenges of modern society organisations are becoming more complex, and so too are the occupations that support them, including the Corporate Security occupation. Within this complexity progression is a changing security environment that impacts business opportunity and societal expectations due to a shift away from risk acceptance (Beck, 1992). Subsequently, the study investigated the Corporate Security stratum of work within large organisations in order to understand career opportunity, complexity, and influence within the context of the socio-organisational literature. By grounding the study in the underlying theory of Jaques' (1996) work into General Managerial Hierarchies, the study took a broad view on the Corporate Security stratum.

The study consisted of two phases, with the first consisting of online surveys distributed to four Australian organisations (N=53), and the second consisting of semi-structured interviews and focus groups with individuals from three Australian organisations from various hierarchical seatings (N=15). Key findings included an identified Corporate Security stratum that stretches from Stratum One through Stratum Four (out of Seven strata), with a postulated occupational progression ceiling at Stratum Four. Further, this progression ceiling is the likely outcome of the role of Corporate Security within organisations; namely as a technostructure function that supports business decision making but does not directly influence profit-making activities. Corporate Security appears to be bounded in specialised problem solving. Further, the study supports the literatures articulation of Corporate Security roles, however, it contests the articulation of the Corporate Security strata within organisations—finding limited support for executive security roles.

COPYRIGHT AND ACCESS DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) Incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher degree or diploma in any institution of higher education;
(ii) Contain any material previously published or written by another person except where due reference is made in the text of this thesis; or
(iii) Contain any defamatory material.
(iv) Contain any data that has not been collected in a manner consistent with ethics approval. The Ethics Committee may refer any incidents involving requests for ethics approval after data collection to the relevant Faculty for action.

Name Codee Roy Ludbey

Signed 

Date 1 May 2019

ACKNOWLEDGEMENTS

To my supervisors, Dr. Dave Brooks and Dr. Michael Coole; thank you for all the support through the years.

To my partner in life, Letesha, thank you for putting up with the entire process from start to end.

To my work colleagues and particularly my employer and professional mentor, Shane Norton, for supporting me throughout this endeavour. Thank you.

To those key individuals who facilitated access to their organisations and let me ask questions of them and their teams. Thank you.

Finally, an acknowledgement to the Australian Government, for their support through the Australian Government Research Training Program Scholarship. It definitely made life much easier!

TABLE OF CONTENTS

FIGURES

CHAPTER ONE

INTRODUCTION

1.0 Introduction

Corporate organisations are becoming more complex to meet the challenges of modern society, and so too are the occupations that support these organisations (Oesch, 2015; Stichweh, 2008). Within this complexity progression is a changing security environment that impacts business opportunity, societal investments, and incentives for those entering the workforce; particularly when considering the continued societal movement towards risk reduction and risk identification. As articulated by Beck (1992) as a described risk society, manufactured risks are becoming less acceptable with time, and organisations are adjusting to suit this societal risk tolerance (Willis, 2007). Nevertheless, while many demonstrate the link between the capacity of individuals to manage complexity (Jaques, 1996; Le Grand & Tahlin, 2013), uncertainty and to forecast future trends with occupational progression, the impact of modern technology has substantially reduced the time available to make decisions, and allowed individuals to collect more information than ever before, arguably changing the equation for occupational success (Craddock, 2002; Le Grand & Tahlin, 2013; Maitland & Sammartino, 2014). Subsequently, the impact of such changes has substantially shifted the perception of occupations and their role within organisations; in particular when it comes to managing risk and conducting profit making activities. Structured hierarchies are giving way to more ad-hoc and flat organisational structures (Clement, 2015; Ivanov, 2011; Robbins & Judge, 2012).

Considering the rapid change in organisational structures, approaches to market, and the workforce that fulfils the required roles to carry out organisational objectives, one must consider how emerging professions may succeed where traditional approaches may no longer apply (Oesch, 2015; Speer, 2017). Where profit making activities are seen as essential in modern capitalist firms, competing priorities for social, ethical, and moral impacts of business are taking larger parts in organisational direction (Clarke, 2015). Such changes result in uncertainty about future roles, careers, and pathways to senior executive levels; ceilings of career progression that have existed in the past could be shifting, and new ones being put in place in response to market demands (Freidman, Laurison, & Miles, 2015; Koch, Forgues, & Monties, 2015).

Nevertheless, for the security practitioner and those who fulfil roles within the security occupation in large corporate enterprises, the existence of such a ceiling seems very real, and a clear hindrance to their success (Fay, 2002; Ludbey & Brooks, 2017; McGee, 2006), however to others, this ceiling does not exist at all (ASIS International., 2004; Cubbage & Brooks, 2013; McKinley Advisors, 2018). The

essence of this dichotomy is influenced by a substantial number of possible factors, including those alluded above, and warrants investigation. Where occupational ceilings exist, they should be challenged on the basis of the occupations merit and influence on organisational objectives, which is, in part, what this study seeks to explore.

1.1 Background of the Study

The stratification and differentiation of individual labour within modern capitalist societies has led to a wide variety of specialised occupations—each with their own jurisdictional boundaries, areas of influence, and relative importance in the corporate organisation (Abbott, 1988; Strauss, 1975/2001). Typically, those occupations that closely align with the profit-making activities of their employer have substantial influence in the labour market, while those who support these activities rather than take a direct part have less power in their career prospects (Sammarra, Profili, & Innocenti, 2012; Speer, 2017; Weeden, 2002). In review of these supporting functions, some appear to attain more career success than others, with this distinction in relative importance often not explored (Heslin, 2005; Koch et al., 2015). Nevertheless, these factors and several others affect individual career progression and wage growth over their careers even in the face of occupational upgrading, often without realising the underlying factors influencing this reduced growth (Oesch, 2015). Consequently, it is interesting to explore where occupational ceilings exist, particularly where such occupations play a non-trivial role in allowing the organisation to carry out its activities unhindered.

It is suggested that Corporate Security is one such specialist occupation; it's sphere of influence, resourcing, and hierarchical peak can be limited within organisations according to some (McGee, 2006; Smith & Robinson, 1999), and to others, it has a position of equal importance to some profit making or directly related activities such as accounting, finance, and marketing (ASIS International., 2004; MacCallum, 2013). This dichotomy of views will be explored in further detail in the following sections, however suffice to say that the security occupation is a non-trivial one within Australia and around the world (Prenzler, Earle, & Sarre, 2009). The practice of Corporate Security is ever expanding and being considered more important in the face of modern societal threats (Gill, Taylor, Bourne, & Keats, 2008), and therefore deserves investigation into the potential limitations in security careers for practitioners.

1.2 An Overview of Corporate Security

Corporate Security as a practicing occupation is considered an entity, public or private, that provides for the self-protection of an organisations people, information and material assets (Cubbage & Brooks, 2013; Sennewald, 2011; Walby & Lippert, 2014). In Australia, although the size of the security practice is hard to measure due to the lack of resolution found in the official data sources, Steden and Sarre

(2007) suggest that there are over 90, 000 Corporate Security workers. Such a base of economic employment suggests that the provision of self-protection in Australia is a major expenditure, and the Australian Security Industry Association Limited (2017) estimates that between 2012 and 2013, $4.9Bn were spent on private security. These costs, incurred by Australian citizens, corporations, and other entities resulted in the provision of security workforce services and security electronics to protect themselves from harm.

Subsequently, large corporations incur significant portions of these expenses. However, unlike other security users, corporate organisations have the capacity to employ security staff internally to reduce reliance on such contract services (Gill & Howell, 2014). Such an idea is generally termed 'Corporate Security' and is in most instances considered an independent business function, providing a range of internally focussed services and roles for the management of security threats that pose an intolerable risk to business objectives (Brooks & Smith, 2012).

The concept of a Corporate Security business unit was discussed by the early industrialist researcher Fayol (1916/1949) who articulated such an internal protection function as core a business activity, carrying significant importance within every organisation. He argued for security operations to be embedded within all aspects of organisational work to improve efficiency and reduce opportunity for criminal actions to impact business operations. Today, Corporate Security forms part of many organisational hierarchies, but is not always considered an important contributor to organisational objectives, nor is it deeply embedded across all organisational work structures (Grobler, 2005; Lippert & Walby, 2014; Ludbey, 2016; Petersen, 2013; Walby & Lippert, 2014).

Corporate Security activities, like all occupational work, are aligned along a hierarchical stratum of positions and roles (Jaques, 1996). Such roles, like all other occupations, are embodied within society, determined by specialisation of jurisdictional activities, and reinforced by capitalistic goals such as profit (Brooks & Corkill, 2014; Durkheim, 1993). The significance of any occupation's work in society is determined by numerous factors, and ultimately leads to the development of an occupational stratum (Dillon, 2013). Such a stratum is generally organised in line with perceived societal value, which is articulated through the fulfilment of tasks in the pursuit of occupational goals. The pursuit of these goals is undertaken within entities generally labelled as organisations. Litterer's work defined organisations as a "social unit within which people have achieved somewhat stable relations (not necessarily face-to-face) among themselves in order to facilitate obtaining a set of objectives or goals" (1963, p. 5).

A review of the security literature indicates that the current academic understanding of the Corporate Security's stratum of work is embedded within most corporations' functional activities. Many authors

are considering the stratum of security activity through the context of Corporate Security objectives, making it difficult to clearly identify or articulate jurisdictional boundaries for roles within the domain (Barefoot & Maxwell, 1987; Fay, 2002). A review of the literature suggests significant dissention on role articulation, particularly as each author tends to operate within their own distinct sub-set of the security domain and attempts to classify the strata according to their lived operational area (Craighead, 2009; Fay, 2002; Sennewald, 2011).

For example, the Interim Security Professional's Taskforce (2008) outlined six individual security roles articulated along a stratum, each with rising complexity and time span of horizon scanning. Such an articulation included the most senior function of a 'Chief Security Officer'. This outline of security works, while consistent with such authors as Bamfield (2014) is in direct contradiction with Smith and Robinson (1999) who articulate only four independent functions within a security work hierarchy, reaching its peak at the general (non-executive) management level.

The conflict goes much deeper, with Gill et al. (2008, pp. 14-16) stating that security practitioners cannot speak the language of business and suggesting that there is a general lack of security practitioners who can operate strategically; particularly within today's corporate setting. They go further, presenting findings that suggest security is considered by non-security executive directors to be important to the business, but identifying that senior security personnel lack the business nous to identify, accept, and leverage this perception.

Curiously, earlier findings presented by Nalla and Morash (2002) outline a professional security function that is operating at the heights of the corporate executive, having transformed from a military and policing focussed occupation to a truly transversal business one. MacCallum (2013) agrees with such a view, suggesting Corporate Security is transversal across organisations, as well as operating at the executive stratum.

Nonetheless, despite its business role in managing the threats which pose a risk to organisational objectives, and the clear value proposition of having a well-developed Corporate Security function (Cubbage & Brooks, 2013; Fayol, 1916/1949), practitioners within this occupational stream appear to reach an occupational progression ceiling. McGee (2006) suggests that the business value of Corporate Security practitioners is perceived as a low-level managerial role, as opposed to a role undertaken by educated persons who demonstrate critical thinking and significant business acumen. This perception is contested by Gill et al. (2008) and Gill and Howell (2012), however it could be argued that while societal incentives to undertake security roles clearly exist, perhaps on balance society in all parts of the world do not yet value the input of security professionals within a corporate setting.

Furthermore, the notion of a security executive is articulated within the Corporate Security literature (Cubbage & Brooks, 2013). Such a practitioner operates at the board level of corporate organisations, carrying substantial benefit to an organisation, and demonstrating significant societal worth (Bamfield, 2014). However, findings presented by Ludbey (2016), were consistent with work conducted by Smith and Robinson (1999), Fay (2002) and McGee (2006), indicating that this role may not be normal business practice, but rather the exception. Consequently, the premise of a Corporate Security occupational ceiling has mixed support. Such opposing views are indicative of an environment that does not acknowledge the application of a sophisticated body of knowledge to achieve its objectives, or perhaps a society that does not incentivise or reward the pursuit of such a specialisation.

Such literature conflict has led some authors, such as Hayes (2003) to lament the lack of rigorously gathered empirical data to answer some of the most fundamental questions of the security domain. Therefore, it is suggested that an objective analysis of organisational security roles must take place from an alternative perspective to provide a comparative review of roles across sub-discipline security roles to appropriately articulate an overall stratum of work that is typical between organisations (Ludbey, 2016, pp. 50-53).

1.3 The Research

The study sought to investigate the Corporate Security stratum of work from the sociological, organisational, and career literature using a deductive approach; as opposed to other inductive investigations into the Corporate Security work stratum that have been conducted from the security literature frame (Hayes, 2003). Thus, the study sought to identify and embed an overarching theory of work hierarchies into the research to align Corporate Security practitioners with other work functions to enable a realistic comparison between traditional work structures and the Corporate Security occupation (Jaques, 1996). Subsequently, the study presented a comprehensive review of the sociological, organisation, and career literature, and then turns to Corporate Security as a specialty, technostructure function embedded within this broader literature. Such an approach grounds the research and provides a more independent study of the function to occur.

Subsequently, the research question for this study is: To what extent, if any, does the Australian corporate environment have a career progression ceiling for security practitioners? The research question is further supported by two sub-research questions (SRQ1) What is the corporate stratum of security practitioners in the Australian organisational context? And (SRQ2) To what extent does the Corporate Security function permeate throughout organisations?

1.4 Significance of the Research

The study seeks to investigate the existence of a career ceiling within the Corporate Security occupation, and in doing so, address previously identified literature inconsistency between the socio organisational and security literature bodies (Ludbey, Brooks, & Coole, 2017). Such an investigation is significance as the exploration of security careers within large Australian enterprise will improve academic understanding of the functional significance of security, alongside industry expectations of security careers and how individuals may maximise their career growth (Sammarra et al., 2012). Importantly, such an investigation will improve the security literatures understanding of the stratum of security work, which includes role articulation and responsibilities; supporting future research and contributing to the evolving discipline of security science (Hayes, 2003). Moreover, such findings, generated from a deductive, as opposed to inductive approach, will seek to begin resolving the conflict between the security and socio-organisational literature in terms of the peak security role positioning within organisation; should it be an executive function or not (Nalla & Morash, 2002). Finally, this investigation will influence security education and provide greater insight for educators as to what level of education should be targeted to whom in the occupation.

1.5 Overview of the Study

The study consisted of two research phases that were designed to investigate the research questions as posed in the previous sections. These research phases were specifically considered within a carefully prepared research frame; encompassing an underlying theory to ground the research in sociological first principles, and then a detailed review of the security literature to orient the research process through an understanding of the current literature perspectives. Subsequently, the research process was framed through an understanding of society, human organisation, occupational work within such organisations, and finally, those security activities that occur within the Corporate Security occupational stream.

Therefore, the study consisted of eight Chapters including this Introduction, each focussing on a discrete component of the work. For clarity, The Chapters were summarised below for reference to articulate the overall approach and key topics of each Chapter.

1.5.1 Chapter Two: Society, Organisation, and Work

Chapter Two presented the underlying theory for the study, including the conceptualisation of modern capitalist society, the role of corporate organisations within such a society, and subsequently the activities of occupations and professionals within these organisations—termed work (Clement & Clement, 2013; Strauss, 1975/2001). Thus, the study identified career progression factors, including class, education, and experience. Such factors were further analysed alongside approaches to

measure them in individual work (Jaques, 1996). The Chapter then highlighted how these metrics could contribute to a study of career progression.

Subsequently, The Chapter highlighted the structure of organisations in accordance with the conceptualisation by Mintzberg (1980), which includes the technostructure, support, strategic apex, middle line, and operating core positionings. Such a conceptualisation of organisation is supported by Jaques (1951, 1996, 2002), who included seven layers of work within organisational structures, each with an increasing time span of discretion – the capacity for individuals to make decisions in the face of increasing uncertainty and time forecasting. This decision-making uncertainty is paired with risk management activities undertaken by workers at all levels of work, and specifically within the security domain (Ludbey & Brooks, 2017). Overall, The Chapter creates a framework through which the literature review (Chapter Three) and the following investigation can be oriented and theoretically supported.

1.5.2 Chapter Three: Security as Specialised Work

Chapter Three, continuing from the previous Chapter, articulates the existence and importance of the occupation of security within organisational work. The Chapter elaborates on the literature understanding of such an occupation, including its expected roles and functions within the corporate environment. Importantly, The Chapter delineates the difference between safety and security practitioners, and defines a working jurisdictional boundary between private security, national security, and Corporate Security (Prenzler, 2005) to orient the study through the subsequent data collection and analysis phases.

Further, The Chapter articulated a theoretical work hierarchy structure for security works through the synthesis of the literature discussion, and highlights areas of contention and misalignment with the broader socio-organisational literature. Accordingly, The Chapter presented a view on security career progression within corporate organisations. Some authors suggest that security has opportunity to reach the apex of corporate organisations (Wakefield, 2014), where others have identified hinderances to such progression (McGee, 2006).

1.5.3 Chapter Four: Methodology

Chapter Four presented the study methodology. The method was devised through a pragmatic research lens, which resulted in a qualitative mixed-method approach (Collier & Elman, 2008). The methodology provided robust reliability and validity due to the cross-comparative nature of the devised phases. The first phase consisted of online surveys to determine participant levels of work and most common role taskings. The instrument used in the first phase was developed in previous research (Ludbey, 2016). Subsequently, the outcomes from the first phase informed the creation of a

focus group questionnaire instrument, for use in the second phase. Such an approach allowed for the second phase findings to reinforce or challenge findings in the first phase (Worren, Moore, & Elliott, 2002).

The Chapter further presented the targeted research population and sample, delimited by Corporate Security practitioners operating within Corporate Security functions for large Australian organisations. For the first phase, a population of N=368 was targeted for online surveys, with each organisation (N=4) being purposively selected, with a response rate of N=53 achieved. For the second phase, a population of N=20 was targeted, with N=6 focus groups and one semi-structured interview occurring, and a total of N=15 participants.

Overall, The Chapter articulated the research approach to controlling reliability and validity concerns in sociologoical research, as well as a detailed overview of the data collection method and data analysis method. The articulation of this approach was braced by ethical considerations.

1.5.4 Chapter Five: Phase One

Chapter Five presented the data, analysis, and interpretation of Phase One. The survey data is tabulated and presented for each participating organisation, with an articulated work hierarchy for each. Subsequently, data were analysed statistically for reliability and validity, and an overall work stratum for Corporate Security was uncovered (Field, 2013). Four organisations participated in the phase, where Organisation One operated in the retail sector of the Australian labour market, Organisation Two was a large Australian national banking institution, Organisation Three was a significant private defence industry organisation, and Organisation Four was a gaming and entertainment organisation. Three of the four organisations were listed on the S&P/ASX100, with fourth being listed on a significant international European exchange.

The phase uncovered a peak security position at Stratum Four, with several hypotheses for such a ceiling across organisations. These hypotheses included: the capacity for Corporate Security practitioners to manage uncertainty outside of their domain specialisation (Maitland & Sammartino, 2014); the overall occupational success of Corporate Security within organisations (Freidman et al., 2015); the impact of organisational structure limitations (McMorland, 2005); the complexity of the investigated organisations, particularly within the context of international operations (Clement, 2015); and the influence of organisational compression, where roles are highly responsive and thus have difficulty operating within the strategic sphere (Ivanov, 2011). These hypotheses informed the Phase Two research instrument for further investigation.

1.5.5 Chapter Six: Phase Two

Chapter Six presented the data, analysis, and interpretation of Phase Two. A total of six focus groups and one semi-structured interview were undertaken with 15 participants, with each being presented in The Chapter with their organisation and education and experience background. Further, The Chapter presented the focus group data in summary, with responses articulated against each question asked in the interview process. While not presented in The Chapter, interview data was transcribed and then analysed and coded (Stewart, Shamdasani, & Rook, 2007). The raw interview data, including coding and tabulation were presented in Appendix E and Appendix F. Subsequently, from these question responses and coding processes, themes emerged and were highlighted and discussed in more detail throughout The Chapter.

The major uncovered themes included occupational success, organisational complexity, and progression ceiling. Each major theme had subsequent minor themes identified which are also presented in The Chapter. These minor themes included focus areas such as dealing with uncertainty in decision making, the importance of higher education in career progression, career progression opportunities and barriers, as well as the value of security as perceived by the participants. Nevertheless, The Chapter presented the reliability and validity considerations for the results, with a researcher bias statement provided (Qu & Dumay, 2011).

1.5.6 Chapter Seven: Interpretation and Discussion

Chapter Seven presented the interpretation of the phase findings and subsequent discussion responding to the research questions. This presentation included the response to SRQ1: What is the corporate stratum of security practitioners in the Australian organisational context? where the uncovered Corporate Security work hierarchy was discussed. In response to SRQ2: To what extent does the Corporate Security function permeate throughout organisations? The Chapter outlined the understanding of Corporate Security role complexity, and the application of security works within the broader organisation. Finally, in response to RQ1: To what extent, if any, does the Australian corporate environment have a career progression ceiling for security practitioners? the Chapter articulated an uncovered Corporate Security occupational ceiling and postulates several reasons as to why this ceiling exists within Australian organisations. Subsequently, The Chapter presented these findings within a defined underlying theory and literature framework.

1.5.7 Chapter Eight: Conclusion and Findings

Chapter Eight presented the conclusions and overall findings of the study, including the implications for industry, and academia. The Chapter discussed theoretical implications of the study findings and identified several underlying assumptions within the security literature that are challenged from the

socio-organisational literature. Subsequently, the findings had implications for industry, including practitioner career directions and choices, as well as for the structure and configuration of Corporate Security teams within large organisations. Finally, The Chapter closes with recommendations for future research and a discussion about study limitations.

1.6 Conclusion

The Chapter presented the background to study, being a developed specialist function of Corporate Security within large organisations in line with the differentiation of labour over time. This specialist function provides organisations with the ability to protect itself from harm through the identification, assessment, and management of security uncertainty and security risk. Nevertheless, while it is accepted that Corporate Security roles exist within organisations, it is unclear as to their progression opportunities, career ceilings, and overall stratum of work. Therefore, the study sought to investigate these phenomena through a sociologically grounded approach; using the organisation and career literature as a lens to investigate the security function. Subsequently, the Research Questions are posed, and the significance of the study presented. Importantly, the study seeks to address a previously identified literature conflict between the broader socio-organisational literature and the security literature. Finally, The Chapter provides an overview of the following Chapters, orienting and guiding the reader.

CHAPTER TWO

SOCIETY, ORGANISATION, AND WORK

2.0 Introduction

Chapter Two presents the underlying theory of the study; outlining how society, organisation, and work inter-relate. Importantly, The Chapter provides the context surrounding occupations and their hierarchical structure within society in alignment with a Webian world view (Weber, 1947). Fundamentally, organisations within a capitalist system seek to meet the demands of the market, and do so through specialisation (Smith, 1775/2007). It is this specialisation that led to distinct occupations and later, professions (Wilensky, 1964). Integral to the study of the stratum of Corporate Security roles is why some occupations are positioned in higher order positions than others, and how specialised functions fit within a broader organisation. In the aim of understanding these concepts, a way of measuring the stratum of work was needed. Jaques (1996) presented such a measurement system, and this system is articulated in The Chapter. Finally, the Chapter enshrined these sociological perspectives into a coherent foundation for this study to understand the Corporate Security stratum of work. In support of this foundation, an overview of the organisational system is detailed, providing a framework for Chapter Three to articulate Corporate Security as a discrete, specialised occupation within large corporate organisations.

2.1 Organisation and Society

While there are many theories and philosophical views on what society is and how it is structured, the substantially different viewpoints and systems of understanding lend a picture that is incomplete and only an approximation. In light of this approximation, several theories are interwoven to build a picture of society and organisation. According to Durkheim (1893/1984, p. 79) society is an amalgamation of systems, each consisting of various institutions, organisations and individuals who align with a cultural and social consensus. Simply put, society consists of individuals and groups who agree, or largely agree with a common set of values or cultural norms.

Nevertheless, this body of literature acknowledges that conflict in such values, norms, and goals will always exist within these societies. However, a sociological frame of thought is that a society, whom relies on a market economy, will be able to resolve such conflicts through the behaviour of a free market of both goods and services, and ideas (Friedman, 2002; Mill, 1869; Smith, 1775/2007). Consequently, the market economy does not just resolve conflict in societal goals, it is indeed a inherently motivating factor for goal creation, with the individual pursuit of profit, prestige, and social capital driving both societal expectations and goal setting (Smith, 1775/2007; Weber, 1947).

2.2 Societal Work and Goals

Such motivating factors are key ingredients within organisations, as the individual pursuit of profit, status, and social capital inevitably leads to the creation of these organisations to multiply labour efficiency and pursue societal objectives within the market economy (Brickley, Smith, & Zimmerman, 2009; Weber, 1947). Subsequently organisations, consisting of numerous individuals pursuing the same or similar goals, can be defined as "a social unit within which people have achieved somewhat stable relations (not necessarily face-to-face) among themselves in order to facilitate obtaining a set of defined objectives or goals" (Litterer, 1963, p. 5). These objectives or goals can range widely, from a small team or business units' goal of reducing overhead expenses, through to an executive manager's decision to branch out into a new state or market segment. Extrapolating to the macro of such objectives leads to a picture of numerous individuals exchanging their time and effort in pursuit of profit or outcome within a market economy.

However, not all organisations are directly motivated by profitable objectives, for example charities or state institutions. Yet such organisations do fall within the overall set of systems which make up the entity of society (Parsons, 1951). For instance, within the societal entity, Parsons (1951) argues that there are four distinct sub-systems which allow society to function. First, there is the economic system, which drives societies capability to adapt to changing circumstances—the market. Second, there is the political system, which sets overall societal goals, and through democratic (or other) processes, allow individuals to influence the way in which these goals are attained—the social consensus. Third, the legal system which regulates how these sub-systems and individuals interact, with a strict code of conduct and guidelines to integration between these, themselves and the individual. Finally, the Cultural system provides an overall reference point for individuals, or, more specifically, a function of 'pattern maintenance' to restrict the rapid change an uncontrolled economic system would bring – the cultural consensus.

Within such a societal framework, organisations are geared to be as efficient as possible. Several organisational methods have been suggested for maximum efficiency, including bureaucratic, voluntary, authoritarian, and self-serving organisational types (Robbins & Judge, 2012). Each organisational typology has its strengths and weaknesses, but all have to find a niche within the market economy while aligning with societal and cultural norms to achieve their goal of profit generation (Krugman & Wells, 2006) or other objective. Nevertheless, each of these organisation types require specialist functions fulfilled by individuals with their own economic value accrued through experience, education, and other sociological factors.

2.3 Specialisation and Incentives

Early work by Davis and Moore (1945) examined the role of individuals within such societal systems. They argued that specialisation in the market leads to a rise of different organisations in different market segments. Such differentiation of organisations within markets is generally supported by the economics literature, and within these organisations, there is inherently a specialisation of talent or individual work (Smith, 1775/2007; Webster, 2001). Davis and Moore (1945) thus considered that the distribution of individuals in societal hierarchies can be explained by the inducement of individuals into particular roles through motivation and desire. In particular, the inducement created by providing access to sustenance and comfort, humour and diversion, and self-respect and ego can significantly motivate individuals to set particular goals. For example, Parsons (1951, p. 26) stated that such goals may include the attainment of particular social or occupational status within a peer group or society at large (Parsons, 1951, p. 26). Extending this argument further is Barnard's suggestion that the importance a particular role plays in society leads to significant inducements for individuals who wish to attain such status; those who are employed in such roles are inherently located higher on the societal hierarchy than those who are not, with associated compensation and authority (Barnard, 1938/1971, pp. 127-138).

Dillon (2013, p. 173) highlighted that such positions along the social hierarchy are ranked unconsciously by society in terms of their importance, complexity, and training required to fulfill the role (Dillon, 2013, p. 173). Inherently, a nominal level of skill is required to perform the duties of any organisational or societal role, and this requires both natural capacity, as well as education and training. It would hold then, in the face of continuing labour division and specialisation (Durkheim, 1893/1984), the more complex society becomes the more complex the roles required to sustain the market are required. Wilensky (1964) considered this in terms of professionalisation, where the specialisation and prestige of the role shifts from a mere occupation to a fundamental societal role.

Abbott's (1988) work articulated that as occupations become professions they become highly compensated and respected specialities and move towards higher restrictions for entry, such as requiring a minimum level of education, a particular societal standing or class, and other professional restrictions (Abbott, 1988). Such pre-requisites allow society to restrict and control those who are operating at the higher levels of society to be only those of 'fit and proper' character; bestowing some level of prestige and inherently incentivising individuals (Krugman & Wells, 2006), ultimately, professionalization is about the social control of expertise (1988).

2.4 Class and Structure

Unsurprisingly, this stratification in society, alongside the societal restriction of progression formed a class based stratified system, where some individuals and organisations are elevated above others based on a variety of factors. Importantly, such elevation is a concern as individuals below those in a superior position generally have no opportunity to progress beyond their existing status (Dahrendorf, 1959). For instance, Marx and Engels (1848/1963) identified several class indicators, including education, birth right, money, and societal authority. When applied to occupations, several studies including the works of Marx and Engels (1848/1963), Weber (1947), Dahrendorf (1959), and McGregor (1997), have found that class plays a significant factor in career progression, compensation, and societal standing (Freidman et al., 2015).

Drawing on this body of literature the stratification and class structures found within the occupation hierarchy, particularly within profit seeking corporate organisations is of particular importance. It could be argued that the occupation-profession divide is one such class differentiator within capitalistic systems. As Webster (2001) discussed, scarce and desirable labour attracts the highest use, and thus the highest price; scarcity is artificially introduced by professions and thus segregates high value work into an untouchable class separate from the 'common' occupations (Abbott, 1988). Webster (2001) suggests that the scarcity of the individuals labour includes the ability to learn, deal with uncertainty, make decisions, and organise people. In a broader context, professional segregation, individual class background, and other such indicators associated with career progression (Le Grand & Tahlin, 2013), what emerges from this discourse is a stratum of work.

When investigating occupational or professional roles within a stratum of work within capitalistic organisations, it is important to consider such class factors (Weeden, 2002). Freidman et al. (2015) suggest class factors such as birth right, financial security, and education directly correlate to the probability of an individual reaching the peak of an occupational work hierarchy. In the Australian context, McGregor (1997) identified that education is one of the most significant class mobility factors. Therefore, to ascertain the extent to which occupations or professions (i.e. the security occupation) permeate throughout an organisation to influence or control activities, these underlying factors need to be reviewed.

2.5 Stratification and Success

Acknowledging such class structures, Heath (1981) identified that individuals can further be stratified along other inherent societal hierarchies, including status and authority. In this sense, an individual can be born into a higher class, yet achieve little status or authority through their chosen occupation, or vice versa. Heath (1981, pp. 140-150) contended that education is one of the most influential

factors able to shift an individuals' occupational standing and perceived professionalism and is a key aspect in class mobility. Such views are reinforced widely in the broader literature (Freidman et al., 2015; Le Grand & Tahlin, 2013; Speer, 2017). Furthermore, education has substantial impact on an individual's first job, which has carry over effects for the rest of their career (Speer, 2017).

Heath (1981, p. 167) suggested that status in modern society is legitimised through actual achievements that are socially acknowledged (Heath, 1981, p. 167). Such legitimisation suggests that individuals who do not follow high status professions and seek occupational employment in non-traditional roles may have difficulty breaking unconscious perceptions within society in terms of the value judgement (Friedson, 1984). Such a claim is important, as there are inherent restrictions on individual attainment of peak organisational roles. If the individual is already working against societal norms due to occupational choice, other factors such as education, experience, birth right, and money will collectively influence that individual's status attainment, particularly within the work hierarchy (McGregor, 1997, pp. 30-35).

McGregor's argument is supported by Freidman et al. (2015) who found that those of lower class in the traditional sense do not progress to the peak of the professional work hierarchies. In fact, even when entering highly restricted work professions within the apex of societal worth, individuals from a lower-class educational background received lower compensation on average than their higher status peers (2015).

Furthermore, such high-ranking positions within society should be considered 'professions' which, as Torstendahl (1990) argues, are roles where individuals use their knowledge and skills as social capital, as opposed to pure problem solving or occupational oriented tasks (Selander, 1990). Interestingly, the prestige associated with professions is not dependent on the individual to solve problems, but rather their ability to exclude others from practicing within their jurisdictional boundaries (Abbott, 1988; Torstendahl, 1990, pp. 3-6).

Collins (1990b) went further, suggesting that professions also have a felt identity, which leads to this 'status group' effect. Inherently, professions are not merely occupations that have removed competition through the defence of esoteric jurisdictional boundaries, but rather, they have a 'calling' or societal honour attached. Fundamentally, a perception of altruism and sacrifice accompanies the professions, leading to the associated respect and appreciation that leads to the higher social standing (Wrzesniewski, McCauley, Rozin, & Schwartz, 1997).

Wilensky's (1964) seminal works argued that not all occupations can become professions, with which Collins (1990a, pp. 13-14) agreed, suggesting that professionalization rests on the capacity for the occupation to gain meaningful power in society. Such power aligns with the concept of authority, and

thus can be aligned with education and social standing in society (McGregor, 1997). Further, to attain societal power, Collins (1990a, pp. 17-18) argues that the formation of a self-regulating community that can push for total autonomy of management is vital. Broadly speaking, professions are considered 'socially idealized occupations organized as closed associational communities' (Collins, 1990a, pp. 17-18). As Wilensky noted, technical knowledge is not enough to become a profession, the social organisation of these occupational groups is a more significant influencing factor (Wilensky, 1964). With the appropriate organisational structure, professions can restrict the supply of their esoteric knowledge, reinforcing market scarcity to favour their inherent specialisation. Ultimately, professions become credentialed groups who forms a governing class in society that controls knowledge, as opposed to the means of production (Murphy, 1990, p. 71).

Some have argued against this conception of professionalization, with criticisms of the self-imposed restrictions on occupations being easily overcome by an individual who learns the appropriate expertise and ignored credentials in favour of practical on the job experience (Friedson, 1984). Such arguments fall short however, when it is noted that not everybody can specialise in everything; leading Grusky and Sorenson (1998) to argue that the conception of professionalization as outlined above is critical to understanding social class, occupational division of labour, and modern capitalistic society. This view is significant given the ability of professions to also exclude practice from those who do not hold that requisite credential (Wilensky, 1964).

Such discussion results in the conception that the perceived societal value of an occupation results in its ability to restrict entry and progress up the organisational hierarchy. If the occupation is perceived as functionally important to the betterment of society, it can attain profession status, leading to further societal rewards and a more authoritative and powerful place along the work strata. This view is important when considering the roles and responsibilities of the Corporate Security occupation within society; while not yet a profession, it perhaps has the potential to become one (Coole, Brooks, & Minnaar, 2017).

2.6 Typical stratified work specialisations and organisational structures

Organisations are inherently specialised to meet the demands of their particular market segment (Scott & Gerald, 2007). However, within this market specialisation, every organisation must employ staff of similar occupational undertakings no matter their particular market focus. For example, oil and gas extraction organisations are just as in need of human resource management professionals as technology companies, or retail organisations (Brickley et al., 2009). Such typical occupations within an organisation hierarchy tend to support the core business function which results in profit making activities (Mintzberg, 1980).

Mintzberg's work highlighted such a position. This body of work considered common ability across four broad organisational roles, as outlined by Mintzberg (1979, 1980, 1989); the strategic apex, the middle line, the techno structure and the support staff. According to Mintzberg, the strategic apex consists of those executive strata workers who set strategic direction and are responsible for outlining policy and long-term decisions for the future of the firm (Jaques, 1996). The middle line is synonymous with middle management and is typically those individuals who have some specialisation but are mostly responsible for directing business units of specialists to achieve their profit-making activities; translating strategic direction to achievable goals for the operating core (Craddock, 2002; Sadler-Smith & Shefy, 2004). The techno structure consists of occupations and professions who apply their specialist skills to the design and maintenance of the organisation, helping the executive strata make decisions to adapt the organisation to its operating environment and market place (Brickley et al., 2009; Galbraith, 1985; Sammarra et al., 2012). Finally, the support staff are those roles that provide indirect support to the organisation by way of special services on an ad-hoc basis. Importantly, the fifth organisational role, the operating core is responsible for-profit making activities and is directly responsible for producing the goods, services, or other such productive work to sell to the market. Such articulation is depicted in Figure 1. Figure 1 highlights that such roles in the operating core are mostly specialists that align with the firms' specific market segment, while the other four are more common amongst all corporate organisations.

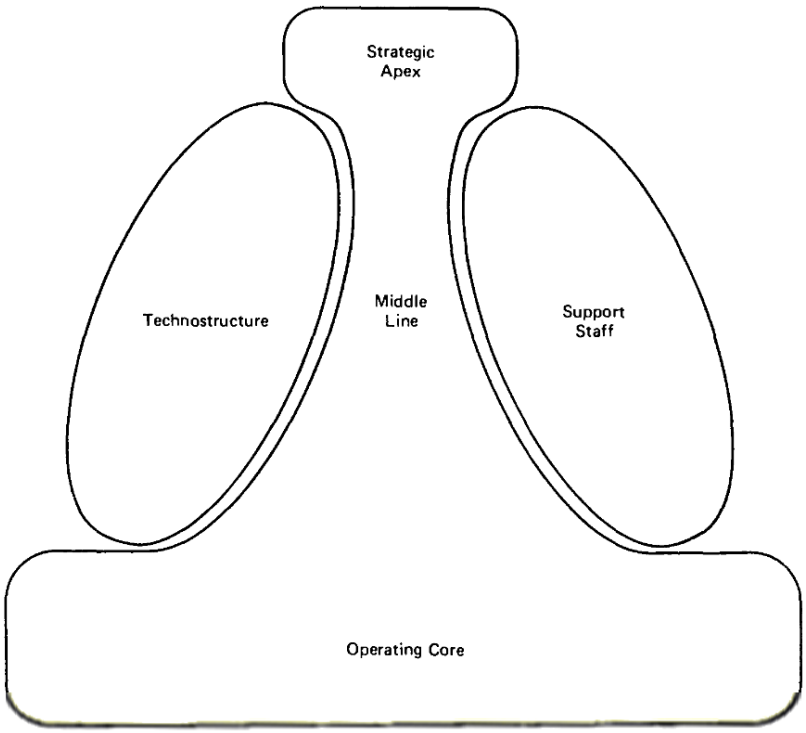

Figure 1. General Framework of Organisational Forms (Mintzberg 1980; Martin & Fellenz, 2010)

It is important to note that this structure largely holds true for the majority of organisational structures; including the simple, beuracratic, and adhocracy structures.

2.7 Organisational Progression

Within these supporting and profit generating structures, career progression opportunity may vary. Early investigations into career progression by Strauss (1975/2001, pp. 139-145) indicated that as an organisation matures, so too does the movement and progression within the enterprise; stabilising along defined pathways. These defined pathways can have pre-determined termination points at various levels of the organisation, with the majority of careers ending at the middle management level. Progression pathways into the executive strata are rare and highly sought after, leading to significant competition.

Strauss (1975/2001) and Holland, Sheehan, Donohue, Pyman, and Allen (2012, pp. 122-134), suggest that highly specialised work functions have fewer options to progress hierarchically within organisations. What stands out is that lateral movements throughout an organisation and across skill sets leads to a higher likelihood of progression up the organisation strata of work, rather than the maintenance of highly specialised work (Jesus, Seibert, Kraimer, Wayne, & Liden, 2015). Mumford, Campion, and Morgeson (2007) reconcile this by explaining that higher positions along the corporate strata of work require broader and more general skill sets, which would logically be developed through a multitude of lateral movements within an organisational structure (Koch et al., 2015).

2.8 Measurement of Stratification in Work

While there is a broad literature on job analysis and its relation to organisational hierarchy and progression systems (Brannick & Levine, 2002; Brickley et al., 2009; Marsden, 1999), few theorists attempt to measure work and its role in organisational stratification. Such measurement would allow a more objective approach to identifying individual capability and roles fit, as well as provide a measure of role hierarchy. Furthermore, such an objective measure of work stratification would lend some capacity to consider the broader implications of organisational stratification, role hierarchy, societal value and an individual's career decisions; providing a framework to understand occupational progression.

Subsequently, through several decades of investigation, the seminal work of Jaques (1951, 1996, 2002) developed an approach to measuring both occupational roles within corporate enterprises, as well as individual alignment to such roles and their placement along a clearly delineated and structured strata of work. Interestingly, this stratification measurement system is equitable across all organisational types (Grobler, 2005), as it measures the inherent human capability to undertake work

through a considered review of judgement and uncertainty management (Bazerman & Moore, 2009), as opposed to other subjective measures.

Jaques (1996), argued that by observing an individual's time span of discretion, one can determine their relative position along an organisational hierarchy, which is supported by Ivanov (2011). Discretion in this instance is considered the individual capability to exercise judgement in making decisions to carry out a task over a period of time. Task complexity is also a factor defined as the time-span of discretion for a task (judgement over time), paired with the complexity of the task (difficultly and uncertainty), can be considered indicative of the level of work for a role (Ivanov, 2011; Jaques, 1996; Lee, Rainey, & Chun, 2010). As Jaques states "complexity may be defined in terms of the number of variables that have to be dealt with in a given time in a situation, the clarity and precision with which they can be identified, and their rate of change" (1996, p. 64).

Jaques' (1951,1996,2002) influential body of work demonstrates that such complexity, tied with the individual's time-span of discretion provides an objective measure of the level of work within a role, and enables for unbiased comparison between roles. To determine the task-time of a role, it is necessary to explore the roles responsibilities, determining which task, or task sequence has the longest target completion time. This task is the measure used to determine the level of work required for the role within the stratified system.

Later, Le Grand and Tahlin (2013) came to a similar conclusion in their work investigating the work hierarchy from an entirely different perspective. Typically, skills and authority are the central dimensions of labour stratification and progress along these dimensions, which as previously discussed can be influenced through further education, skill development, or other human capital investments. Further, people who are able to learn, manage people, and make unsupervised and sophisticated decisions while facing uncertainty and non-routine circumstances, are the most likely to progress along the hierarchical work strata (Webster, 2001). Le Grand and Tahlin (2013), based on this understanding and a review of sociological class theory, suggest that the productivity of an individual can be measured as follows:

$$P = E \times C$$

Where productivity (P) is equal to the product of an individual's effort (E) and capacity (C) in a role. Furthermore, they argue that the employers aim to attain maximum return from their employees (Rate of employment profitability, or R) can be considered as the difference between the workers productivity (P) and their wage (W):

$$R = P - W$$

Or, substituting the productivity equation above:

$$R = (E \times C) - W$$

Finally, by considering that effort in a role would be maximised through incentive schemes (assuming optimal employer strategy), one can reduce the employer's return calculation to:

$$R = C - W$$

As demonstrated above, a core component of the wage-profitability calculation is the employee's capacity to conduct the work. Interestingly, from an analysis of empirical data in response to this theoretical formula, Le Grand and Tahlin (2013) argue that efficiency related considerations are the key differentiator in hierarchical positions along the stratum of work. Such a review of productivity aligns closely with Jaques (1996) understanding of the work equation.

2.8.1 Uncertainty, Capacity, and Risk

With regard to individual capacity to undertake work within the bounds of operational uncertainty, it is likewise considered that these concepts relate to an individual's capacity to manage risk (Ludbey & Brooks, 2017). Risk, as discussed by Fischhoff, Watson, and Hope (1984) includes the management of uncertainty through consideration of various consequences of a decision, technology, or otherwise, alongside their likelihood of occurrence. Slovic, Peters, Finucane, and MacGregor (2005) explain that this decision making and risk consideration is not always rational, and can be affected by personal feelings and biases. Nevertheless, risk decision making is inherently related to work capacity as articulated by Le Grand and Tahlin (2013), the time span of discretion and uncertainty management as articulated by Jaques (1996) as each relies on the management of risk to inform their work activities across an identified work stratum.

2.8.2 The Work Stratum

In review of these concepts, a generic stratum of work is identified in relation to this increase in capacity within corporate organisations and is outlined in Table 1 with each identified stratum detailed in the following sections. Such a stratum seeks to provide a framework through which the study of Corporate Security can identify and categorise security roles within organisational structures.

Table 1

Occupational Stratum of Work in Organisations

Stratum	Time-Span of Discretion	Role Complexity	Employee Role
Seven	20+ Years	Extrapolative Development of Whole Systems	CEO
Six	10 – 20 Years	Defining Whole Systems	Executive Vice President
Five	5 – 10 Years	Shaping Whole Systems	Business Unit President
Four	2-5 Years	Transforming Systems	General Manager
Three	1 – 2 Years	Task Extrapolation	Unit Manager
Two	3 Months – 1 Year	Task Definition	First Line Manager
One	1 Day - 3 Months	Concrete Shaping	Front Line Worker

*(*Adapted from Jaques, 1986, 1996)

2.8.3 Stratum One: Concrete Shaping / Direct Action

In accordance with Table 1, Stratum One work consists of tasks that require no abstract thinking and that fall within a heavily prescribed routine (Jaques, 1996). For example, direct action work has a prescribed output, such as manual labour tasks or production line work. Rowbottom and Billis (1977) explains that work at this level can be demonstrated once and applied to various situations through the application of training and procedures. Where work falls outside of these procedures, supervisor input is needed, or the employee undertakes a simple trial and error approach.

Consequently, work conducted at this level including decision making and forward thinking is between one day and three months. Decision-making in Stratum One roles consists purely of deciding on the appropriate application of procedures or training to achieve the highly defined tasks specified by a supervisor (Clement & Clement, 2013).

2.8.4 Stratum Two: Task Definition / Diagnostic

This level captures employees in supervisory and first line managerial roles that require some discretionary thinking but are still bounded by policy and procedures are considered Stratum Two roles (Clement & Clement, 2013). While work at this level is not wholly prescribed, discretionary decision-making is limited to between three months and one year. Importantly, Stratum Two workers can interpret cumulative information along a linear path of progression. Individuals at this level of work can further self-reflect and forecast into the future, identifying problems before they occur and take steps to manage these problems (Jaques, 1996).

An example of such a role would be a manager forecasting resources by way of producing shifts or schedules for workers over several months, ordering in stock for a store, or managing the installation of new equipment as part of a technology upgrade prescribed by higher order strata. Furthermore, individuals that fulfil Stratum Two work can also consist of specialist professional roles such as engineers, and graduates (Jaques, 1996).

2.8.5 Stratum Three: Task Extrapolation / Alternative Serial Paths

Continuing on from Stratum Two work, Stratum Three roles deal with more work complexity. For example, individuals at this level of work need to be able to manage future obstacles and situations through the management of several serial processes (Jaques, 2002). In practice, this means that individuals working in a Stratum Three role must develop new systems and procedures which prescribe the way future situations will be handled, and this includes defining the work that needs to be conducted by Stratum One and Stratum Two workers to achieve business objectives (Jaques, 1996).

Stratum Three workers possess the capacity to direct their judgement of a situation through a diagnostic accumulation of information forecasted between one and two years into the future. Such judgement allows the individual to change direction of a project or projects to an alternative if required and still deliver the outputs required (Grobler, 2005).

Individuals operating at Stratum Three are thus generally considered as fulfilling systematic service provision roles such as senior or chief engineers, doctors, and lawyers (Rowbottom & Billis, 1977; Jaques, 1996). Alternatively, they could be considered a specialist manager for a sub-discipline within a business unit (Ludbey & Brooks, 2017).

2.8.6 Stratum Four: Transforming Systems / Parallel Processing Tasks

Forecasting further into the future requires a shift from direct management tasks towards general management activities (Mumford et al., 2007). Typically, this means a move away from specialist and technical tasks towards more business focussed activities such as managing individuals, finances, and implementing broader business objectives. Consequently, individuals in Stratum Four roles should be able to influence the processes that allow the implementation of strategic objectives set by those above (Jaques, 1996). Importantly, this influencing of implementation requires the individual to develop several pathways to achieve several independent goals. For example, managing multiple independent projects with a finite amount of human and other resources to share between each.

Individuals at Stratum Four while managing multiple projects simultaneously, must also manage a number of subordinates who are each working towards their own goals along their own separate pathways (Clement & Clement, 2013). Consequently, Stratum Four workers must have the ability to

guide these separate paths and provide alternatives where required. This work is achieved over a time-span of discretion between two to five years, and typically constitutes the role of a general manager (Gould, 1986; Jaques, 1996).

2.8.7 Stratum Five: Shaping Whole Systems through Direct Action

Where Stratum Four workers consist of general managers, Stratum Five workers are within the executive stream of organisations (Clement, 2015). They are responsible for managing business units, ensuring consequences of their decision-making and direction are managed both internal and external to the business unit. Importantly, Stratum Five individuals should account for second and third order consequences from their decision making. Such foresight requires individuals to sense the inter-connection between tangible and intangible variables (Ivanov, 2015a).

Importantly, individuals at Stratum Five are responsible for recruitment and training strategies. This includes shaping the business units' approach to market, and to some extent the service offering provided (Jaques, 1996). Due to the nature of such activities, the role is focussed on managing uncertainty between five and ten years into the future, while adjusting the internal posture of the business unit to meet shifting market demand over this time period.

2.8.8 Stratum Six: Defining Whole Systems / Conceptual Abstract

Stratum Six work is considered to operate entirely external to organisation business units with considerations to broader interactions between the organisation and the political, technological, social, economic and intellectual external environments (Jaques, 1996). Consequently, individuals must be capable of shaping and influencing these environments in line with the organisations' strategic goals, contributing to the long-term survival of the organisation in the marketplace. Stratum Six work requires resilience and the capacity to implement long term strategies over 10 to 20 years.

Work at this level is generally aligned to Vice Presidents of an organisation, with responsibilities ranging from developing external professional networks, managing corporate investment priorities, and running multiple business units to meet market demands and ensure core business outputs meet the strategic vision of the organisation (Clement, 2015).

2.8.9 Stratum Seven: Development of Whole Systems through Extrapolative Development

Stratum Seven work is abstract by nature, resulting in significant uncertainty and complexity for decision making. Importantly, decisions at this level of work influences the overall organisations ability to understanding, and meet the societal needs expressed in the marketplace (Papadakis & Barwise, 2002). Roles at this level pursue multiple world-wide strategic plans, including alternative pathways to achieve these plans to satisfy the marketplace.

Such work is generally enacted over a period exceeding 20 years, with international capital, human, and asset resourcing. Therefore, individuals at this level of work must be able to grapple with the complexities presented by the global marketplace and make decisions that can interact with the uncertainty presented to the organisation (Clement & Clement, 2013).

Stratum Seven individuals are considered to be the apex of an organisation, operating as the executive leadership with ultimate responsibility for all decisions and actions undertaken. Jaques (1996) considers this role to include a fundamental understanding of generational thinking, with plans being developed and implemented for the next generation of customers. Appropriately, the responsibility for the development of Stratum Five business units through in-house development, mergers, acquisitions or joint ventures rests at this level of work (Jaques, 1996).

2.9 Strategic Decision Making / Work Hierarchy Decision Making

In review of the work hierarchy outlined in the preceding sections, what emerges is that decision-making capability changes substantially along the strata of work. Strategic decision-making occurs at the executive levels of an organisation and generally involves dealing with substantial uncertainty and limited information (Mumford et al., 2007) directed towards future business objectives. This work is in contrast to the lower strata of work that are delegated responsibility for enacting strategies to fulfil strategic decisions by undertaking tactical and operational level decision making activities (Ivanov, 2015b).

Importantly this delegation of work based on strategic decision making does fundamentally affect the long-term operational capacity of the organisation, and significantly influences the roles that are created to fulfil the strategic vision (Ivanov, 2011, 2015a). As such decision making is generally aligned to profit making activities, specialist functions are typically excluded from such decisions, but rather feed into the decision makers understanding of the operating environment and their forecasts (Papadakis & Barwise, 2002; Papadakis, Lioukas, & Chambers, 1998).

Bazerman and Moore (2009) articulate the holistic consideration of uncertainty by executives. They detail that the management of uncertainty at the higher reaches of organisations occurs with less specialisation; specialists feed into the decision-making process, however the executives generally synthesise these various specialist streams to make decisions in review of a broader uncertainty picture. Such a view is reinforced by Maitland and Sammartino (2014), who outline that deep specialisation restricts an individual's capacity to deal with uncertainty outside of their area of expertise. Such restriction is severely limiting to strategic decision making, but is highly useful for tactical and operational decision making (Mumford et al., 2007).

2.10 Conclusion

The Chapter introduced the underlying theory of work stratification and specialisation within societal systems, as well as the theory of managerial hierarchies. These theories collectively identified factors that are influential in the progression of individuals in their careers and these may be even more influential in specialist careers. Corporate Security roles sit within a broader organisation, but are highly specialised, however, their place within organisations can vary based on the size and risk tolerance of these organisations (Brooks & Corkill, 2014). To understand Corporate Security and its facilitator role in achieving organisational objectives, a deeper investigation within the broader organisational stratum is required.

To understand the broader organisational stratum, the Chapter presented the underlying theory of the study, that being the sociological theory of differentiation, paired with the general theory of managerial hierarchy; each expounding on the sociological factors that lead to organisation, specialised work, and goal achievement (Durkheim, 1893/1984; Jaques, 1976). Primarily, it is proposed that organisational hierarchies are developed in response to social cues such as status attainment and monetary reward within the context of achieving mutually agreeable objectives. Within these objectives, various occupations are developed to meet sub-objectives.

These occupations lead to specialised work hierarchies within organisations that are stratified according to an individual's capacity to conduct work in uncertain conditions (Jaques, 1996; Le Grand & Tahlin, 2013). Subsequently, these stratified positions are defined, oriented, and directed by strategic decision making occurring at the executive level. Such specialist hierarchies include the roles of Corporate Security practitioners, which are discussed in detail in the following Chapter.

CHAPTER THREE

SECURITY AS SPECIALISED WORK

3.0 Introduction

As articulated in the previous Chapter, the creation of organisations provides a vehicle through which individuals can come together to pursue goals in society (Litterer, 1963). These goals can be profit driven, or otherwise, but result in the exchange of labour for other goods and services (generally a wage). Nevertheless, organisations face difficulty in the pursuit of their goals with interaction between the various systems within society leading to conflict. For example, the production of goods or the provision of services to the market requires various types of individuals with different skills and abilities (Robbins & Judge, 2012).

Subsequently, for organisations to successfully pursue their goals, they must employ a variety of specialists to fulfil tasks that sum to the conduct of their business. These specialists tend to align (excluding managerial ranks) to either technostructure roles, support roles, or operating core roles. One of these specialists is the security role. The security role within an organisation would be considered a technostructure role that shapes the organisations operating environment to be free from harm (Ludbey et al., 2017; Wakefield, 2014).

While the security occupation is broad, it is functionally significant, and is evidenced by early managerial theory (Fayol, 1916/1949). Nevertheless, due to its specialised nature and non-operating core positioning, questions arise to the occupation's permeability throughout the organisational ranks, particularly at the apex of corporate organisations (Brooks & Corkill, 2014; Mumford et al., 2007).

Therefore, The Chapter presents the contextual focus of the study, outlining security as an occupational stream within corporate organisations. Through the application of the previous Chapters underlying theory, this discussion was framed to highlight the relevance of the security function within corporate organisations, as well as its impact on corporate activities. Importantly, the stratum of security work was considered, particularly where there is disagreement within the security literature around how this stratum emerges in practice. Various security roles are identified, and a typical security function articulated. Overall, The Chapter articulates that while there is agreement that security is important and expected within organisations (Gill & Howell, 2012), it may yet have become a profession and as such, may not be operating as expected within the executive stream.

3.1 The Practice of Security

Security is a broad discipline encompassing a significant number of tasks and functions ranging from risk management, through technology, physical security, business continuity management, personnel security, industrial security, fire and life safety, intelligence, investigations, law, criminology, safety, and facility management (Brooks, 2013; Griffiths, Brooks, & Corkill, 2010). Consequently, the definition of security is often debated, and varies depending on context. When considering the application of security across the individual, group, and national contexts, often the requirements, outcomes, and objectives of security change, highlighting this contextual nature (Smith & Brooks, 2012, p. 7). Therefore, a definition for the purposes of this thesis was considered.

One definition of security is that of "a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury" (Fischer, Halibozek, & Green, 2008, p. 31). In this definition, the focus on individuals and groups leads to an implication of a predictable environment for organisations to operate without disruption and harm. Where Fischer does not differentiate safety and security, Somerson (2009, p. 5) does, articulating the difference as the protection against duncery, as opposed to the protection against a malicious action. Such a separation resonates with Fayol (1949), who defined security as the protection of property and persons and delivering peace of mind for an organisation and its employees.

Where a clear link between the application of security and the protection of organisations can be drawn, the practicing area of this overlap is considered Corporate Security. Such a corporate stream of the security occupation consists of consultants, managers, and investigators to name but a few (Bamfield, 2014). These practitioners are focussed on providing a self-protection function embedded within an organisation that aims to reduce the risk of harm to people, information, and physical assets from a threat (human) actor (Brooks & Smith, 2012). Such a function, according to Burnstein (1978) is one of a purely protective function focussed on the provision of physical security elements such as a guard force, alarm systems, and locking devices. However, the modern implementation of security services includes higher order risk mitigation strategies, incorporating planning and forecasting that encompass all organisational operations (Bamfield, 2014). Consequently, the jurisdictional boundary of Corporate Security can be hard to define due to its far-reaching influence on several disparate managerial and operational specialities (Coole et al., 2017).

As evidence of this difficulty, sub-groups within the self-protection stream i.e. the protection of organisations, exist that would not distinctly be considered Corporate Security. As articulated by Prenzler (2005), these streams are private and Corporate Security; where private security practitioners

provide contracting and outsourcing services, and Corporate Security practitioners render in-house services to organisations. As argued by Brooks and Smith (2012), there is overlap between these practicing sub-groups in terms of their applied context; however, both groups tend to have authority at the community, organisation, group, and peer levels of security application.

Nevertheless, while Brooks and Smith (2012) outline other sub-groups within the security occupational stream, including police, military, and government employees, these sub-groups are distinct from corporate and private security sub-groups due to their orientation towards national security activities as opposed to the self-protection of private organisation or individual property (Prenzler, 2005; Sarre & Prenzler, 2000).

Therefore, the practice of Corporate Security appears to be limited to the in-house services offered by a department or division within an organisation for the self-protection of its assets. These services, fulfilled by both operational and managerial staff include the application of physical security measures such as locks and guards, but also higher order risk management strategies. It is argued that Corporate Security is an applied management context, particularly at the higher strata of work. Consequently, Ludbey (2016, p. 21) defines Corporate Security as:

> "The protection of business operations from disruption and harm, including; people, information, assets and reputation through procedural, technical, and physical risk mitigation and control measures."

Importantly, such a definition captures the business imperative for the in-house provision of security and aligns Corporate Security outputs with the direct mitigation of security risk. Such an alignment is important, as Corporate Security is considered a technostructure function—one which shapes the operating environment for the business, reducing its risk exposure in the process (Ludbey et al., 2017).

3.2 Occupational Significance

While there is no denying that security as an occupational stream, whether in the private or corporate sub-groups, is recognised by organisations (Gill et al., 2008), there is debate around its overall significance to organisational activities. The security industry in Australia, for example consists of over 120,000 individuals, with an annual turnover of approximately $8Bn, with $4Bn being in the manpower sector, and $4Bn being in the electronic security sector. However, this measurement of the industry only consists of those members in the technical and security guard force occupations including alarm installation and maintenance, monitoring of CCTV equipment, security patrols, and alarm response (Bergin, Williams, & Dixon, 2018, pp. 8-9).

Prenzler (2005) examined the Australian security industry, as presented by the Australian Bureau of Statistics (ABS) 'security provider' classification for census data (Table 2). According to Prenzler, the census data does not collect information on Corporate Security practitioners and is focussed on operational security functions such as locksmiths, security officers, and other such roles. It is recognised that this study into security roles only identified those in the lower strata positions, as more senior security roles are likely to be classified as professional staff (Ludbey, 2016). Further, those identified in the census through Prenzler (2005) work are licensed operators providing a third-party service, whereas many in the security professional staff within corporate organisations do not need a security license, restricting the opportunity to accurately measure the industry in Australia and thus not fully reflecting the scope of security activities and roles (Brooks, 2014, pp. 697-699).

Table 2

Security roles as outlined by the Australian Bureau of Statistics

Private Investigator	Bailiff/Sheriff
Security Advisor	Security Officer
Locksmith	Armoured Car Escort
Insurance Investigator	Security Guards/ Security Officers
Debt Collector	

(Adapted from Prenzler, 2005)

Nevertheless, the security occupation has grown according to economic predictions of supply and demand; specialised work in this market segment has evolved more sub-disciplines over time (Krugman & Wells, 2006). Based on the technical and guarding proportion of the security industry in Australia, security is clearly significant from an industry perspective. Thus, the premise that the managerial stream is similarly significant is proposed.

Subsequently, from a societal perspective, some would argue that the growth in the security industry is in excess, with the security conversation leading to societal harm through the restriction of freedoms (Freeman & Freeman, 2008; Lippert & Walby, 2014; Molotch & Molotch, 2012; Neocleous, 2000). One argument is that security has paired with the conception of the risk society, as another pursuit of risk reduction from all possible harms (Beck, 1992). Such a pursuit has led to the unnecessary and ill-justified intrusion into modern life, including mass surveillance, reduction of privacy, restriction of free movement, and massive bureaucracy to enforce a ‘permanent emergency’ (Marcuse, 2006; Neocleous, 2006, 2007). Consequently, large sums of money, time, and human

resources are being spent to little overall effect in aid of allaying poorly defined fears regarding safety (Krahman, 2008; Molotch & Molotch, 2012).

Nevertheless, others suggest that the security occupation is a fundamental requirement for a functioning society (Petersen, 2013; Simonsen, 1996). Where national security agencies seek to protect the state from trans-national threats, in the modern threat environment they rely more on the private provision of security to protect the homeland (Gill & Pythian, 2006; Petersen, 2014). Such roles and responsibilities being fulfilled by the private sector could be seen an overall public good, resulting in a safer society for all (Bilgin, 2003). Importantly, where some restrictions have been placed on society, the resultant risk reduction in crime, terrorism, and other disorder is a necessary outcome of protection (Fischer et al., 2008).

Pragmatically, the true benefit or harm of security likely falls somewhere in between these two extremes (Petersen, 2013). The occupation provides, in most cases, a reasoned and rational approach to reducing potential and actual harm to society and could be seen as a net good (Gill, 2014; Gill & Howell, 2012). Noting however, that there are cases of corruption and overreach in the industry, which is expected in any collective human action (Marquette & Peiffer, 2015).

Nevertheless, the occupation tends to view itself as a public good with self-identification as a profession (Brooks & Coole, 2017; Interim Security Professional's Taskforce, 2008); however, as Coole et al. (2017) suggest, the security occupation may not yet be at the point where it could be considered a true profession (Manunta, 1996). Security has progressed towards a role of societal recognition and import but has yet to be conceived into the professional realm due to the inability to compartment itself and define and enforce its jurisdictional boundaries (Gill et al., 2008; McGee, 2006).

From an academic perspective, the function, practice, and theoretic of security has achieved greater significance over time and across all aspects of the domain; however, this interest is relatively new. Subsequently, at times, areas of the domain are ill-defined and lacking in academic rigour. For example, Hayes (2003) articulates that a significant portion of the security literature is non-academic, finding more discussion of security in trade magazines and how-to books than academic journals and texts. Such a lack of academic rigour on the topic has influenced the current discourse in the study of security. Nevertheless, substantial publications have been presented, exploring the depth and breadth of the security occupation since this critique, though Bamfield (2014, p. 791) suggests more investigation by non-security disciplines such as management specialists should be undertaken to provide less insular perspectives on the domain.

3.3 Occupational Worth

As the security occupation matures, its role within corporate organisations expands. For example, Talbot and Jakeman (2009) identify the opportunity for advanced internal security functions to leverage an organizations enterprise risk management framework to transform organisational risk exposure and treatment measures. Rather than simply being considered a cost-centre, security controls could be aligned to the enterprise risk management framework, clearly drawing relationships between security spend and business return by way of extended operations in high-risk areas, reduction in legal or regulatory risk, and other such strategic aims. Such advanced security functions are likely rare, as evidence suggests that internal security teams vary significantly in complexity, impact, and status within organisations (Gill et al., 2008). Such variation in complexity and status leads to differing security approaches throughout organisations, for example, some security functions may be more operational, tactical, or strategically focussed.

The extent of such influence, status, and complexity within organisations depends on several factors. For example, the organisations risk perception, the perceived importance of security risk as opposed to other risk types, and the qualification and skill of the individual responsible for security operations within the business (Gill, 2014). However, the internal security function influences the way in which the organisation interacts with and shapes the environment around it (Ludbey et al., 2017). For example, a loss prevention program influences the interaction between staff, customers, and physical assets, while an electronic security regime shapes business operation both during and after hours by way of restricting access, monitoring public areas, and facilitating responses to incidents (Fay, 2002; Gyarmati, 2004; Ludbey et al., 2017). Such an arrangement closely aligns with the concept of a technostructure function in Mintzberg's articulation of corporate organisation structure (1980). Technostructure functions are seen as business enablers and enhancers, shaping the environment in which an organisation operates, value adding and reducing unwanted risk exposure, even though they are not generally profit-making activities (Clarke, 2015; Galbraith, 1985).

Such a focus for security functions within organisations has significant support from the literature, with many agreeing that security provides numerous avenues through which business can be supported through direct and indirect means (Cubbage & Brooks, 2013; Sennewald, 2011; White, 2014). As Petersen (2013) discussed, the significant literature viewpoints are as follows; Security can be measured in terms of adding value to the bottom line through profit making activities when aligned to an enterprise risk management framework. Or, security adds value through protecting society as a broader whole, playing a part in corporate social responsibility (CSR) obligations. While it is likely that these two viewpoints are not mutually exclusive, they demonstrate the concept of security as a

business enabler in different respects; CSR and Enterprise Risk Management each are responsible for managing the environment in which the organisation operates, and value created through either activity will likely enable further profit-making activities in the future (Krugman & Wells, 2006; Mahajan, 2010). It is important to note however, that both viewpoints have no direct influence on profit-making, and merely influence the risk exposure of such profit-making activities.

The extent of this influence on business objectives and their risk exposure likely varies depending on the security functions mandate within the organisation. Gill et al. (2008) provided a detailed review of how Corporate Security is perceived within organisations by other business areas, which might be considered a proxy for influence. Overall, they found that security was viewed favourably in supporting business objectives and is viewed on similar terms to other business functions such as human resources. They note however, that traditional Corporate Security roles such as physical security are viewed less favourably and as less important than newer roles, such as cyber security. Furthermore, the effectiveness of security was questioned mainly due to the difficulty in having appropriate metrics for the function. Such views lend to the idea of the security occupation being able to provide tangible value to the organisation, without being viewed purely as a cost centre. Nevertheless, in reality the inability to measure the provision of security leads to some organisations not appropriately valuing the provision of security services.

3.4 The Stratum of Security Work

With the articulation of Corporate Security as a business enabler, it is important to understand how such an organisational function is constructed and how it operates within corporate enterprises. As outlined above, the occupation is quite disparate, with many practicing areas of specialisation. Such specialisation is further enhanced through the application of security practice across a substantial number of operating contexts, for example: nuclear security, hotel security, retail security, arts and culture security, stadium security and infrastructure security, to name but a few (Brock, 2008; Loveday & Gill, 2004; Lucier, 1999). The perceived unique requirements of security between industry organisations has led to an ad-hoc and discordant array of roles, functions, and hierarchies across the domain (Ludbey et al., 2017).

Nevertheless, it is argued that the practice of security across its stratum of roles is functionally quite similar between contextual application, with various sub-practices (such as loss prevention) being required in some applications and not others (Coole et al., 2017). However, the literature articulation of these roles is not always consistent (Ludbey et al., 2017).

3.4.1 Executive Security

Nalla and Morash (2002) suggest that security is a relatively senior function, reporting to the executive strata of an organisation. Such senior roles would consist of shaping business decisions through a security lens, allowing the business to operate securely and make decisions informed by security risk (Talbot & Jakeman, 2009). The concept of an executive level security function is supported by Ocqueteau (2012), who suggests that a great majority of security directors for large corporations may have their direct superior in the executive committee. Bamfield (2014) agrees, postulating that such a role—the Chief Security Officer—should exist to develop companywide strategy and policy in the protection of organisations assets and operations.

This executive role is supported by several more literature sources including the Interim Security Professional's Taskforce (2008) in Australia, and Apollo Education Group (2015) in the United States amongst others (Bayuk, 2010; MacCallum, 2013; McKinley Advisors, 2018; Sennewald, 2011). Such a role is considered to be faced with significant uncertainty (Bamfield, 2014; Elenkov, 1997), but is supported by a series of security managers, supervisors, and operations staff to ensure high level security strategies are implemented throughout the organisation (Cubbage & Brooks, 2013).

Nevertheless, Maitland and Sammartino (2014) outline the role of uncertainty in decision making amongst senior executives and high-status decision makers within corporate organisations. They suggest that effective decision makers with influence in organisations are typically more diversified, generalist managers without a deep speciality. Where specialists provide input on strategic decision making they typically only provide comment on their area of expertise and rarely provide insight in other areas. Such discussion suggests that the alignment (or lack of alignment) of the security function to the core business objectives could have a substantial impact on the occupations status and capacity to provide guidance at the strategic organisation level.

Further, Lawler III and Rhode (1976, p. 192), suggests that organisations facing unstable, complex, or uncertain operating environments need to move decision-making authority down to the lower strata of work, as they have a closer view of the information and can act quicker to respond to the changing environment. It could be argued that security operations are highly responsive and require individuals to operate in complex and uncertain environments in their day to day work (Black, 2004; Gyarmati, 2004).

3.4.2 Security Managers

Security manager roles can be responsible for a specific specialist area or several specialist areas (Bamfield, 2014). While security managers are shifting away from a defined specialty (i.e. pure specialisation in investigations) and towards a more generalist managerial role, they are still

generalists within the security domain (Brooks & Corkill, 2014). For example, they may now need to understand company policy, local laws and regulations, the role of security technology, and security operations resourcing and management to name but a few (Barefoot & Maxwell, 1987; Fay, 2002). The security manager is considered a general or middle manager who oversees the specific implementation of security mitigation strategies in their area of expertise. According to Smith and Robinson (1999), this role is actually the peak of the Corporate Security occupation, not recognising the chief security officer (CSO) as a valid positional seating. Smith and Robinson (1999) position is supported by Fay (2002) who also articulates that the security manager is at the peak of the Corporate Security hierarchy. Each of these authors identify operational staff in the security function, including security supervisors and security officers.

3.4.3 Security Supervisors

Security supervisors are responsible for coordinating and organising operational staff who fulfil tasks such as customer service, responding to incidents, or monitoring CCTV (Nalla & Wakefield, 2014). Further, supervisors are expected to ensure security officers remain alert, and maintain the integrity of patrols (Hasan, 2016). Security supervisors are also responsible for human resource management (i.e. setting up shifts, managing training, and disciplining staff where appropriate), managing operational risk, controlling and utilising electronic security technologies, and taking part in investigations (IFPO, 2008). Baker and Benny (2013, pp. 201-218) agree, suggesting that while the duties of the security guard force are dependent on the threats and risks identified, both supervisory and operational roles remain relatively similar.

3.4.4 Security Officers

Security officers fulfil the various roles managed by security supervisors to ensure they are carried out in such a way as to implement many aspects of the organisation's security risk reduction strategy. Brislin (2014) identifies numerous roles fulfilled by these staff, including public relations, physical security, deterrence, operating electronic security systems, observing and reporting incidents, writing reports, patrols, investigations, crowd control, emergency response, first aid, traffic control, removing violent or difficult individuals (including responding to workplace violence), and cooperating with police (Nalla, Johnson, & Mesko, 2009). Fay (2002) suggests that security officers are integral to interrupting criminal acts and lend a significant deterrence to opportunistic crime (Nalla & Wakefield, 2014).

In review of the literature discussion, Figure 2 outlines an example security work hierarchy. The roles identified in this figure have been normalised from the literature, as there is little agreement about

role titles (McKinley Advisors, 2018). These four identified levels of work include two strata of operational roles, and two strata of tactical managerial roles (Ludbey et al., 2017).

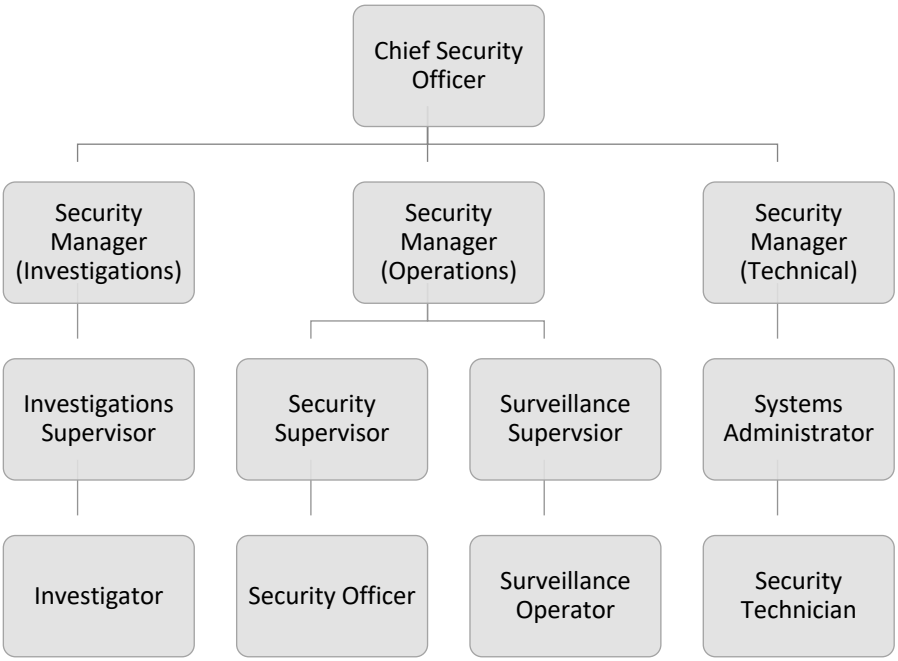

Figure 2. Security Hierarchy (Synthesized from Brooks and Corkill, (2014);Sennewald, (2011);McKinley Advisors, (2018); Ludbey et al (2017))

Overall, while these security roles on first glance seem to stretch the length of a traditional corporate structure, it is suggested that the peak role, that being the Chief Security Officer, is in fact merely a middle management position in the majority of instances (Ludbey et al., 2017). Where this role has been described, its deep domain specialty and limited remit in practice (McGee, 2006) leads to characteristics of a general managerial position (Jaques, 1996). Subsequently, such limitations affect the security functions capacity to influence behaviour and permeate throughout the business, reducing its impact in setting direction for the provision of security throughout the organisation (McGee, 2006).

3.5 Security Career Progression

As articulated by Mumford et al. (2007), as an individual progresses in the work hierarchy, generally they require more generalised skills than domain specific skills. Such a view is reinforced by Brooks and Corkill (2014), who posit the same relationship with security career progression. Importantly, the identified roles uncovered in the security literature point to a specialised work stream with some progression towards generalist skills at the peak; however, it is argued that these roles still require strong domain specific skills (ASIS International., 2004). Where Chief Security Officer roles exist, the literature suggests that they are domain focussed and responsible only for areas that align to the protection of the organisation, unlike other executive roles that may be responsible for multiple,

disparate departments. For example, the Chief Operating Officer may be responsible for profit-making activities, as well as the legal team, marketing department, and so on (Robbins & Judge, 2012).

Such a disparity in work hierarchy could result in limited progression opportunities at all levels of the security occupation within corporate enterprise. The literature, as discussed in the previous Chapter, suggests that those with generalist skills are more closely aligned to profit making activities are more likely to progress to senior positions within an organisation than those in specialist areas with limited generalist experience (Speer, 2017). Furthermore, the excess of domain expertise required to reach the senior roles in the security occupation can also stunt individual growth due to the poor prospects for promotion within an organisation. If the peak security role is inherently limiting for future progression due to the specialist skills required, then the mobility throughout the strata will also be inherently limiting. Progression often occurs due to role vacancies, but if the specialisation prevents individuals to move sideways or up within the organisation, less role vacancies would subsequently occur.

Subsequently, research conducted by McGee (2006) and Wakefield (2014) suggest that where some security practitioners have achieved substantial progression and recognition within organisations, others have not. These fortunes are likely paired to the organisation's acceptance of security and their emphasis on managing security risk. Nevertheless, progression within the security occupation could be difficult to achieve in either of these scenarios, particularly for those that are not domain specialists. Where progression within the occupation is restricted for domain specialists, and progression outside the occupation is more restricted to those with generalist expertise, security practitioners may meet a career ceiling across all organisational roles (Strauss, 1975/2001).

3.6 Conclusion

The Chapter provided a review of the domain and practice of security within organisations, specifically where the practice is focussed on protecting people, information, and assets from harm within a self-protection of an organisational lens. Such practice was defined as Corporate Security, and this stream of occupational work was classified as a significant contributor to an organisation's work hierarchy. Nevertheless, Corporate Security as a function is not well defined, with such a broad scope of responsibilities that are often not always encompassed in a security role (Brooks & Coole, 2017). Subsequently, the jurisdictional boundary of security is not well defined, leading to questions about its actual contribution to organisation well-being (Gill et al., 2008; Lippert & Walby, 2014).

Overall however, where corporate organisations recognise security as a contributor, the occupation can be influential and valued (McGee, 2006). Importantly, security, according to Petersen (2013) does provide value and influence through an alignment with the enterprise risk management framework;

allowing business to operate in a resilient way through crisis situations, and by playing a part in corporate social responsibility by reducing the impact of crime and terrorism more broadly when considered from a state protection perspective (Bilgin, 2003).

Consequently, the literature has found that security functions tend to be structured around four typical hierarchical positions, those being the security operator, security supervisor, security manager, and chief security officer. These roles tend to operate under short time spans of discretion (Ludbey et al., 2017), and are highly specialised. Subsequently, these roles could be restrictive to career progression, and not conducive to side-ways movement or promotion into other occupational streams. This restriction is particularly true when considering that other occupations value generalist skills as opposed to domain specialist skills (Mumford et al., 2007).

In review of this specialism, at the more senior ranks of the security occupation it is posited that a career progression ceiling is more likely to occur in this stream of work, both at the senior levels trying to progression beyond security, and to those in less senior ranks trying to move up or sideways. It is suggested that those trying to move into other occupations may lack the generalist skills required, and those attempting to move up will be stymied by the lack of overall mobility due to the former limitations for everyone in the discipline.

CHAPTER FOUR

METHODOLOGY

4.0 Introduction

The Chapter presented the research methodology underpinning the study. The methodology embraced a pragmatic approach to the research, using a multi-phased process to collect and analyse data (Dillon, 2013; Roth, 1987). The research design included individual organisational analysis by way of online surveys (Phase One), supported by a mixture of focus groups and semi-structured interviews to interpret and contextualise Phase One's findings (Phase Two). Such an approach is supported by Creswell (2009, pp. 10-11) who suggests the use of multiple measures to ensure validity and reliability of results in qualitative research.

Subsequently, The Chapter presents the study's targeted research population and sample, included four large Australian organisations and their internal Corporate Security teams. Then, the analytical framework through which the collected data set was subjected to is presented. This analysis framework included methods to assess online surveys to review reliability and validity through statistical measures such as the Spearman Rank Order Correlation and Kruskal-Wallis test, as well as coding techniques for interview and focus group transcripts. Finally, The Chapter also presents a discussion regarding the ethical considerations and the approaches undertaken to reduce ethical exposure in the course of the research are described in detail.

4.1 Study Design

The study was grounded in the research philosophy of pragmatism, which ascribes to the world view of solving a research problem through varied approaches rather than focussing on singular research methods (Creswell, 2009, p. 10). Pragmatic research is committed to responding to the research question through any means necessary, acknowledging the surrounding context in the inquiry rather than removing it. As deliberated by Hausman (1989, p. 125), it is important for research to make "use of whatever tools philosophers of science have to offer that appear to be well made and apt for the job." Such an approach is particularly salient when dealing with sociological, economic, or other such investigations of society due to the complexity associated with distilling investigations down into simple a/b experiments. Expanding on this view, Sims (1996, p. 109) suggested that "where there are few theories, or only abstract and unconvincing theories, available and informal exploration in search of new patterns and generalizations is important." Nevertheless, such investigations should include statistical insights, and as the theories progress, more statistical rigour should be applied (Lazear, 2000).

In light of this literature, the study investigated corporate organisations through a sociological purview, which immediately lends itself to deep complexity in the number of influential variables inherent in the possible data set. For example, different organisations are structured differently, operate in different markets, and are exposed to different cultural, economic, and environmental factors. Rather than attempt to remove these variables from the investigation, the study instead undertook a pragmatic approach, which encourages acknowledging such variables throughout the investigation; seeking understanding as it exists in the world.

Consequently, a mixed method, multi-phased research approach was selected, as it provided a foundation for the study's targeted inquiry. Such understanding is uncovered in a form that provides the best comprehension of the research problem at the time (Collier & Elman, 2008; Creswell, 2009). As Roth (1987, p. 6) states, "we are most likely to do our best (in pursuit of knowledge) by adopting a non-restrictive [sic] view of what to count as a form of rational inquiry." Such a philosophy facilitated the embedding of previous relevant studies within the research design, including Ludbey (2016), Ludbey and Brooks (2017), and Ludbey et al. (2017) to orient and refine the research enquiry. These previous bodies of work articulated an underlying theory of a structured society and a theoretical lens of human organisation, which aligned with the objectives of the study. For example, the research phases of this study were specifically designed to investigate areas of the security function within corporate organisation based off key outcomes of this previous work.

Through designing the study and accounting for previous research in this area, the current body of work was tuned and adjusted to overcome limitations in the previous research. Such concerns included small sample sizes, dissention on the applicability of the underlying theory in modern organisations, and therefore limitations in the instruments used for data collection (Ludbey, 2016). These limitations were addressed in the study through an exploration of recent applications of this underlying theory, a larger and more robust sample, and a comparative statistical analysis of data collected as opposed to descriptive statistics to enhance reliability and validity of findings. Figure 3 presents the study's research design, phases, methods of collection and analysis, demonstrating the significance of the enhancements undertaken in recognition of previous study limitations, resulting in a robust and valid research design.

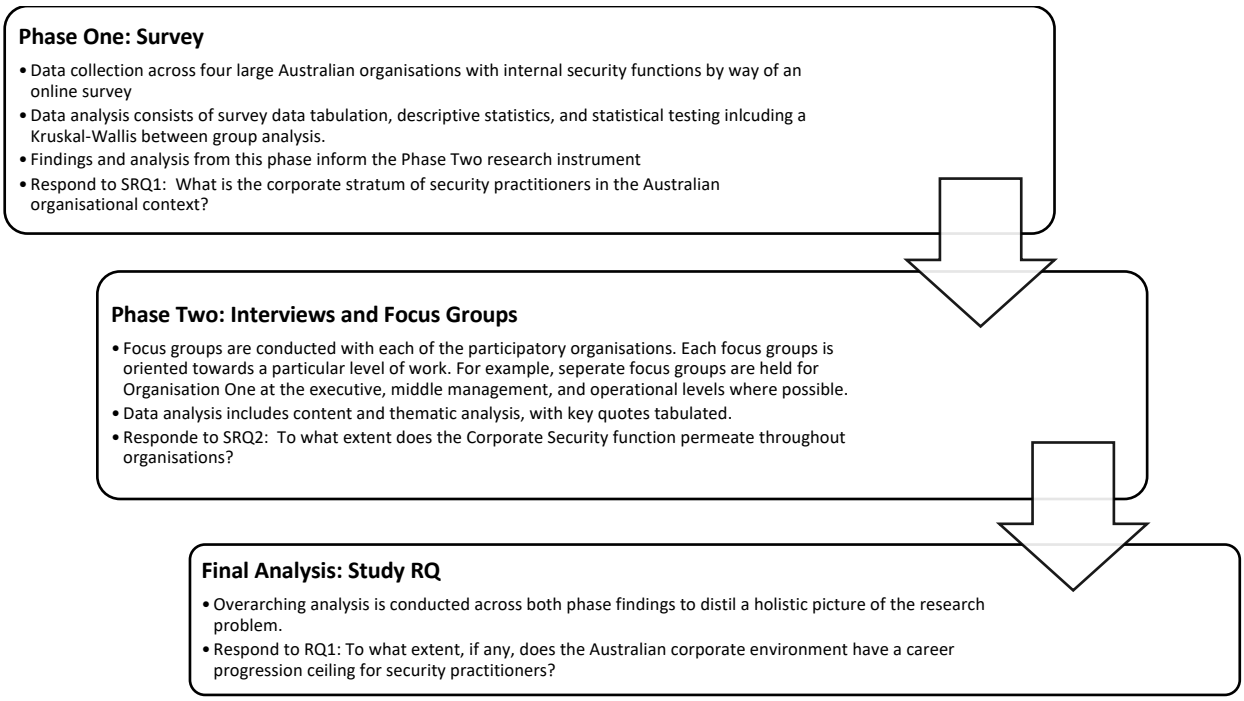

Figure 3. Study Design

Each of the study's phases methodologies provided specific research findings towards responding to the research sub-questions (Creswell, 2009; Patton, 2015) for later interpretaion against the study's research question. Phase One consisted of a cross sectional comparative analysis to provide specific insight into various participating organisations' security functions, their roles and associated levels of work within each organisation (Bryman, 2012, pp. 59, 72). This phase embedded a survey questionnaire developed from Ludbey (2016), which acknowledged the latest findings into the stratum of work, supporting the validity of the underlying theory in modern organisations. The survey questionnaire was distributed to four large Australian organisations with an internal security function, across distinct market segments.

Phase Two undertook a confirmatory analysis using a series of focus groups and semi-structured interviews, drawing participants from Phase One's participating organisations (Brandtnera, Helfertb, Auingera, & Gaubingera, 2015). Such focus groups and semi-structured interviews allowed participants from multiple market segments in different organisations to elaborate on their perspectives and provide insight into the data collected in the first phase. Importantly, as (Denzin, 1989) and Roth, (1987) suggest, focus groups are good for understanding the findings in previous phases of research due to the rich data collected. The focus groups were guided by a semi-structured questionaire developed out of findings from Phase One, with semi-structured interviews following

the same question pattern; ultimately directing data collection towards a deeper understanding of the corporate se curity stratum of work within large Australian organisations.

4.2 Phase One

Phase One of the study undertook a cross-sectional approach to data collection, drawing on a purposive sample to recruit archetypal Australian corporate organisations that have an internal Corporate Security function (Bryman, 2012). The phase sample consisted of four corporate organisations with embedded security functions, where organisational consent to participate was gained, and then employees were requested individually to participate initially in an online survey questionnaire. The questionnaire, developed in previous research, presents a series of questions to participants that uncovers their level of work in their organisational setting (Ludbey, 2016). The distribution of this questionnaire to individual workers in each selected security function provides a snapshot of the levels of work present within that security function and outlines an occupational hierarchy that can be compared to the other participant organisation security functions.

This phase aligned with the work of Bryman (2012, p. 58) who pointed out that a cross-sectional research design is suitable for collecting data from more than one sample at a single point in time to investigate a connection between two or more variables. As sociological research prohibits the manipulation of variables due to the inherent complexity found in society in many cases, cross-sectional research provides an approach through which correlation can be inferred at a point in time. Such a research approach is consistent with other variable rich and contextually challenging scientific investigations such as those found in economics (Krugman & Wells, 2006; Lazear, 2000).

Importantly, this approach enabled the issue of variation in each organisational sample to be adjusted for. For instance, each measured Corporate Security function differed in size and complexity, varying the sample size of each organisation; however, the survey questionnaire targeted the entire Corporate Security population within each case, allowing a review of the occupational stratum at one point in time without having to account for commencements, resignations and dismissals, or other organisational changes.

Furthermore, the research design undertook an investigation of four independent participant groups that were analysed statistically (Greene & D'Oliveira, 2005, pp. 5-10) to uncover significant variation or concordance. As each organisation operated within their own distinct market set, an analysis of each group was conducted individually, and then a between-group analysis was undertaken to uncover relations and significance. Such an investigation provided arguably an objective picture regarding the Corporate Security structural model in a typical corporate organisation distinct from market segment bias or organisational type (Field, 2013, pp. 15-16).

4.2.1 Sample Frame and Selection

The phase sample comprised the four corporate participant groups, with Group One comprising security practitioners from a large corporate enterprise operating in the retail sector of the Australian market. Group Two consisted of security practitioners operating within a large Australian national banking institution. Group Three were security practitioners working within a significant private defence industry organisation, and Group Four consisted of security operators within a gaming and entertainment organisation. Overall, a phase population of N=368 was targeted, with each organisation being purposively selected, and thus subsequently, the participant sample, with a response rate of N=53 achieved.

Due to the comparative, cross-sectional nature of Phase One, each organisation was considered in respect to the independent variable. Further criteria for the sample selection included the requirement for informed consent, an agreement to participate and willingness to share information with the researcher. The participating organisations were large corporate enterprises, considered representative of the broader corporate environment across market segments (Thacher, 2006; Yin, 2014, p. 48). A representative sample is one where the results derived can be inferred to represent the broader community of interest, and as such results are said to be generalizable to this broader population. The sample was considered representative as the organisations selected were some of the largest corporations within their market sector. Consequently, the study aimed to capture data corresponding to typical security functions embedded within large Australian corporate organisations.

In aid of achieving such representativeness, the organisations (n = 4) were required to be:

- a '*large'* organisation (over 100 internal, full time staff);
- listed on the Australian Securities Exchange (ASX) or other international securities market; and
- employed individuals internally in a Corporate Security role within a security business unit.

Participation requirements included employment status, where participants had to be currently employed Corporate Security practitioners regardless of seniority or education within the participating organisations.

4.2.2 Data Collection

Phase One data collection was achieved through the use of a survey questionnaire validated in previous studies, consisting of responses to a distributed online survey (Appendix A). The survey embedded two measurement tools developed in previous research (Ludbey, 2016), namely the Task Complexity Measurement Tool and the Work Measurement Scale. Each participating individual operated within the security function in one of the targeted organisations. Such a cross-sectional

(across market segments and across hierarchies of work), comparative analysis provided an overview of the levels of work within the function for each organisation sample and provided an outline of the types of roles undertaken. Importantly, collected data was initially analysed in Qualtrics, where the survey was constructed. Upon export of the raw data from the Qualtrics web portal, NumPy and SciPy; which are scientific analytical packages for the Python programming language; were used to apply statistical processes to the data.

This approach premised to highlight potential ceilings of progress within the security function for each organisation sample, examining if individuals are performing beyond or below their theoretical hierarchical seating. For example, an individual assessed as having a high level of work being seated in a low-lying position within an organisation may suggest an unspoken ceiling of progression. Once the individual analysis of each organisation sample was completed, a meta-analysis of all samples was undertaken with findings leading to the development of a questionnaire to guide the focus group interviews in Phase Two.

4.2.3 Data Analysis

Data from each organisation sample was extracted from the completed surveys into a csv file and tabulated for analysis through groupings of responses to provide an indication of an individual's level of work. Descriptive statistics including mean level of work were initially calculated, with the variance tabulated to determine the standard deviation of each response. From this calculation, findings were graphed, and the associated error determined. Then a Spearman rank order correlation analysis was undertaken through analytical tools including SciPy and NumPy to provide an insight into the two scales ability to measure the participant's level of work. The statistical analysis facilitated the mapping of organisations security accordant with Jaques' (1996) hierarchy of work, consistent with the previous work of Ludbey (2016) and (Ludbey et al., 2017).

Because each organisation sample is independent and unrelated, and the ranking of individual participants within each sample is ordinal, a non-parametric statistical test was required to determine the significance of any correlation. The Kruskal-Wallis test is suitable for non-parametric data across more than three sample groups, and thus was used in this cross-group comparison (Field, 2013).

4.3 Phase Two

Phase Two of the study used focus groups and semi-structured interviews to uncover the lived experience of security practitioners at multiple strata of work, investigating both the nature of their work and their work hierarchy. Both focus groups and semi-structured interviews were used simultaneously in the second phase as the complexity of organising individuals across organisations, particularly at senior levels, to attend a single location on a specified day proved difficult. To overcome

this challenge, focus groups were conducted with only those within the same strata and same organisation, and where multiple attendees could not be organised (particularly at the executive strata), a semi-structured interview was conducted.

Focus group research includes the use of a purposively or randomly selected number of participants to discuss an area under investigation (Stewart, Shamdasani, & Rook, 2007). For this study, the focus groups consisted of a purposive sample from those organisations targeted in Phase One. The focus groups provided the researcher with a methodology to access participant's thoughts, understandings, and feelings relating to the stratum of Corporate Security work in a way not possible through the survey questionnaire, structured one-on-one interviews, or participant observations. Importantly, focus groups provided context to the survey questionnaire data, accounting for the uncontrollable variables inherent in the design (Sims, 1996).

The study embedded the strength of focus groups in the research as highlighted by Morgan (1997), who pointed out that focus groups enable researchers to clarify or expand on findings from other data collection methods. This view was later supported by Bloor, Frankland, Thomas, and Robson (2001, pp. 8-10), who added that focus groups provide different perspectives or insights into previously gathered data. As stated by Hausman (1989), such data collection methods are important in the type of research this study undertook as it allows contextual data to be collected from which reasoned insights can be gathered without attempting to distil such complex research topics down into a laboratory based experimental setting. Importantly, by combining both the survey questionnaire and focus groups to test initial assumptions regarding the stratum of work in Corporate Security, the study achieved a greater depth of discussion and insight into each organisation and occupational structure. Inherently, this study design provided exploratory findings which could then be tested and confirmed or refuted (Lazear, 2000; Sims, 1996).

The study conducted six focus group sessions, and one semi-structured interview with participants purposively selected through participating organisations by their perceived level of work. Each focus group comprised up to two individuals, with a targeted duration of one hour. Sessions were held in various locations in Sydney, Australia, and some were conducted across regions by teleconference. The focus groups and semi-structured interviews were undertaken within an office meeting room context.

Groups were arranged in this way to provide the maximum possible cross-talk amongst participants, bearing in mind scheduling difficulties and availability of participants. The researcher attempted to avoid individuals sharing a session with their superiors as this could impact the frankness of the discussion and thus limit the richness of the data collected. Furthermore, by grouping participants so

closely to their identified level of work, clear articulation of roles at each subsequent level could be made without having to dissect responses between significant position hierarchy differences in the same group.

In particular, Phase Two enabled triangulation of findings from this phase against the outcomes of Phase One (Denzin, 1989; Roth, 1987). Much like investigating multiple samples to identify the occurrence of a particular phenomenon through literal or theoretical replication, so too, the conduct of focus interviews following the survey phase aids in the analysis (Creswell, 2009). By gathering more data about the Corporate Security phenomenon from another independent data collection methodology, the overall findings of the study were arguably strengthened and therefore more robust (Leonard-Barton, 1990).

4.3.1 Sample Frame and Sample Selection

Phase Two's sample frame required focus group participants to be a currently employed Corporate Security practitioner regardless of seniority or education and be identified as the relevant level of work for their assigned interview group. Overall, a population of N=20 was targeted, with N=6 focus groups and one semi-structured interview occurring, and a total of N=15 participants

Again, participants were purposively selected from those organisations identified in Phase One (Cohen, Manion, & Morrison, 2007). Importantly, participants were selected for their level of work; in the first phase, particular job titles were ranked along the work stratum, which allowed for accurate participant selection while maintaining anonymity for the online surveys. Participants were grouped based on this selection method and assigned to the relevant focus groups (Morgan, 1997, p. 33).

4.3.2 Data Analysis

Data collected through the focus groups were recorded and transcribed verbatim for improved reliability in the results. The data was then subjected to content and thematic analysis through manual coding processes. This method of data analysis is described by Steward, Shamdasani, and Rook (2007) as a means to classify elements of a discussion to probable causes and effects. Accordingly, by focussing on why something was said, meaning can be inferred and analysed in aid of responding to the posed research questions. Thematic analysis is defined as pinpointing, examining, and recording data in such a way as to identify relationships and connections. This approach was used in this study to identify recurring beliefs or explanations about an individuals' work, and the groups understanding of their functional seating along the strata of work. Data was grouped according to question, as per Table 3.

Table 3

Example Data Format for Phase Two

Quote			**Preliminary and Secondary Code**	**Final Code (Theme)**
Work Strata: Operational				
Question Number: 1	**Participant Number:** OYXX	**Example Quote:** "Security is challenging due to the various stakeholders that have to be engage in decision making"	**Example Codes**: Decision Making Stakeholders	**Example Theme:** Work Complexity

Importantly, Braun and Clarke (2008) suggests several steps in the thematic analysis process, starting with transcription, and then coding of the data, which includes tagging key words, then identifying themes and tagging these themes in the data, ensuring they are consistent and coherent. Following this process, the themes are analysed for significance in relation to the research questions, and a clear picture emerges of what the data suggests about the area of study.

4.4 Reliability

Reliability in quantitative research requires consideration of the tools being used to measure the concept under investigation. Such consideration includes the tools stability, or ability to provide consistent results, as well as internal reliability of the tool, which aims to indicate that each item within the instrument measures the same concept, or aspects of the same concept (Bryman, 2012, pp. 168-170). In this study, reliability for the instruments used was based on their valid use in previous research, including a pilot study (Section 1.4.1)

Furthermore, reliability in qualitative research such as focus group interviews has different goals and outcomes as opposed to quantitative research (Merriam, 2009; Patton, 2015). While quantitative reliability is focussed on stability, parallel-forms, and internal consistency, reliability in qualitative research is concerned with ensuring the research approach is trustworthy. Trustworthiness encompasses several elements of quantitative reliability, and in this study, was achieved by implementing a number of procedures, including confirming the accuracy of transcriptions and cross-checking data (Creswell, 2009, pp. 190-193). Importantly, reliability is focussed on ensuring the consistency and repeatability of the research. Reliability was handled in different ways for the various phases and is outlined below.

4.4.1 Phase One: Online Surveys

The research instrument for Phase One was treated as a quantitative instrument, consisting of two tools (the Task Complexity Measurement Tool, and the Work Measurement Scale) measuring at the ordinal level. As such it was measured for internal consistency alongside parallel-forms. Internal consistency refers to the consistency of items on a test to measure a single construct or concept (Christensen & Johnson, 2014, pp. 166-171). Measures of reliability and validity for this survey were considered through cross tool averages and standard deviation elaborated in previous research (Ludbey, 2016; Ludbey & Brooks, 2017). Importantly, such measurement provided insight into the instruments ability to cross check across tools and provided an understanding of the instruments capability to measure the work construct.

Through implementation of the two tools in aid of measuring different indicators or elements of the same construct, equivalent forms reliability and internal consistency were satisfied through score correlation in previous studies (Christensen & Johnson, 2014, pp. 168-169). Finally, a Spearman's Rank-Order Correlation was calculated in this phase to further reinforce the instruments reliability (Field, 2013; Laerd Statistcs, 2013).

4.4.2 Phase Two: Focus Groups

To achieve reliability in focus groups, Stewart et al. (2007, pp. 118-125) suggests using a consistent technique to analyse data across samples. As previously discussed, a consistent analytical approach was used for all participant sample groups (Steward et al., 2007, p. 119). This approach included consistency in the coding methodology. Importantly, reliability in this phase was supported by the findings of the first phase through triangulation.

Transcripts of the interview further provided a measure to improve reliability, as the researcher's interpretation of the data can be reflected upon in light of the raw data (Bloor, Frankland, Thomas, & Robson, 2001, pp. 42-43). Importantly, the moderator of each focus group provided rich, thick descriptions of the interview to aid reconstruction of the surrounding context, allowing the transcripts to be considered appropriately (Creswell, 2009).

4.5 Validity

Validity aims to provide assurance that the data collected throughout the study is useful and meaningful within the context of responding to the research question (Creswell, 2009, p. 149). Validity can be demonstrated in numerous ways, each varying between quantitative and qualitative research. Importantly, validity suggests that research findings are congruent with reality (Merriam, 2009, p. 213).

4.5.1 Phase One Online Surveys

Validity in questionnaire instruments can be determined by the accuracy of the inferences or interpretations one makes from the test scores; in order to be valid, there are many validity tests that can be undertaken for a research instrument (Christensen & Johnson, 2014, pp. 165, 213-214).

One such test is content validity, which refers to the instruments relevance to measuring a particular phenomenon. Content validity was achieved through the use of the Work Measurement Scale and Task Complexity Measurement Tool from previous research (Ludbey, 2016; Ludbey & Brooks, 2015). Past studies such as Laner and Crossman (1976); Laner, Crossman, and Baker (1969), Allison and Morfitt (1994); Allison, Morfitt, and Demaerschalk (1996), and Ivanov (2006) have indicated that Jaques (1996) work is suitable for measuring organisational strata of work. As the proposed instrument has been derived from such literature and used in previous research such as Ludbey (2016), content validity has been demonstrated.

Another test of validity includes construct validity. Construct validity refers to the questionnaire items' indication of the underlying theory or phenomenon being measured (Creswell, 2009, p. 149)**.** The survey instrument was designed through a grounding in the underlying theory of Jaques' requisite organisation, and the broader management literature (Jaques, 1951, 1996; Mintzberg, 1973, 2009; Robbins & Judge, 2012). As the instruments were derived from this literature, and used in previous research to investigate organisational work structures, construct validity has been demonstrated.

4.5.2 Phase Two Focus Groups and Interviews

The role of the moderator in focus group research, and of the interviewer in semi-structured interviews is significant to demonstrate validity (Steward et al., 2007, pp. 80-86), particularly due to potential bias skewing responses. Types of bias that the moderator may bring to the group include personal bias, unconscious bias, and the need for consistency. Such sources of bias can be counteracted through preparation before the interview begins, and being mindful of the types of questions asked, and the responses given to commentary.

Secondly, convergence validity was considered in this study between both phases. Convergence validity is the extent to which two measures or methodologies that provide distinct data are related to one another. While generally considered through statistical correlation tests, convergence can also be considered through a review of the data collected. In this study for example, responses given from the participants in each focus group interview should align with their corresponding assessed level of work in the first phase.

4.5.3 Study Validity

Overall, validity in this study was achieved by using triangulation (Denzin, 1978). As Denzin (1989, p. 234) states, qualitative researchers should seek to examine a problem from as many methodological perspectives as possible to ensure a more accurate measure of the truth. Such an approach aligns with a pragmatic search for the truth, using as many avenues of investigation available to answer the research questions.

Triangulation is explained as the use of different, unique data sources, as well as the collection of similar data between different sample groups, and the collection of data through distinct methods. Such an approach allows for the cross examination of research findings to support various views and to highlight outlying points. Therefore, to ensure a more effective measure of truth in reality, this study used two phases to provide a between method triangulation approach (Roth, 1987; Yin, 2009).

The following measures were used to improve validity in the research:

- The use of several, unique, data sources (Merriam, 2009);
- The collection of similar data between differing organisations (Bryman, 2012; Farquhar, 2012); and
- Two distinct methodological approaches, across two phases (Creswell, 2009).

4.6 Ethical Considerations

The research was conducted in-line with Edith Cowan University's ethical codes of practice, and all participants, organisations, and other parties were made aware of their voluntary status, especially their rights to withdraw, confidentiality of information collected, and anonymity of their individual responses. Subsequently, all organisations and individual participants were required to provide informed consent prior to any data collection (Appendix C). The research was submitted for approval by the Edith Cowan University ethics committee and attained approval before data collection occurred.

Furthermore, the ethical considerations included:

- Participant reflection on self-worth and career prospects post-survey and post-interview;
- Participant opportunity to review interview transcripts after the interview process;
- Participant interaction and opportunity to discuss sensitive matters within a cohort of colleagues and known persons;

The research design catered to these requirements by providing career resources and counselling service information to participants prior to participants, offered participants the opportunity to review

transcripts, and kept focus group sizes small while ensuring that group participants consisted of peer-level individuals with no superiors and their subordinate staff in the same session.

4.7 Conclusion

The Chapter presented the research methodology of the study across two phases, each with their own distinct methodology, data collection and analysis approaches. Such a study design was considered under the purview of a pragmatic approach to responding to the research questions. Such an approach allowed for a flexible research design that maximised the data collection opportunities from the participant sample. The participant research samples for both phases were drawn from four large Australian organisations Corporate Security functions, allowing for cross-sector data analysis.

The first phase sought to understand the hierarchy of security work within the participant organisations, particularly with the view of identifying the maximal strata position of security practitioners. From this hierarchy snapshot, the second phase could be undertaken to more clearly understand the context of such roles along the hierarchy, for example, their influence, capacity to delegate, and make decisions. By combining these two approaches (surveys and interviews), a more robust understanding of the security stratum of work was uncovered.

Furthermore, such a methodology facilitated appropriate control for reliability and validity concerns. By following up data collected through an online survey with a more detailed and data rich interview and focus group process, findings from the first phase could be aligned and cross-referenced with the transcript data in Phase Two. This method is particularly necessary when acknowledging the complexities of collecting sociological data and the inherent background noise that can influence results. The inability to distil the data down to simple concepts and structures under investigation without other confounding variables required rich data to improve confidence. Subsequently, a multi-method approach was used to appropriately respond to the research questions.

CHAPTER FIVE

PHASE ONE SURVEYS

5.0 Introduction

The Chapter presents Phase One of the study, which targeted Four large Australian organisations and their Corporate Security teams. The Phase included the distribution of an online survey to the chosen sample, which included the Work Measurement Scale and the Task Complexity Measurement Tool to identify each participants level of work. The data collected from these surveys was then presented and analysed with descriptive and advanced statistics such as the Spearman Rank Order Correlation and the Kruskal-Wallis Test. These statistical analyses are conducted cross-organisation and cross-measure to demonstrate reliability and validity in the results.

Subsequently, as part of the analysis, some key findings are presented. The analysis suggested that Corporate Security hierarchies are not substantially different between organisational contexts and are limited in hierarchical scope. Consequently, several avenues of investigation are discussed to understand these findings, including the role of occupational success, organisational complexity, organisational misalignment and organisational compression. These avenues are then collated into a questionnaire that directed data collection in Phase Two.

5.1 Participants

5.1.1 Participant Selection

The participant sample was achieved through purposive solicitation of four significant Australian business organisations with an embedded security function. Organisations were approached through professional liaison networks, where a gatekeeper was known by the researcher (Yin, 2014). Each organisation was chosen due to being considered a 'large' enterprise operating within the Australian labour market—three of the four organisations were listed on the S&P/ASX100 list. Interestingly, each organisation operated in a separate market segment, with no overlap in core business operations.

The work measurement instrument was distributed through an established liaison within each organisation—who was generally a senior manager or executive responsible for the security function. The liaison distributed an online web link to their participating employees internally through e-mail. In total, approximately 368 participants were selected across the four organisations to undertake the work measure survey.

5.1.2 Participant Sample

As discussed, the participant sample consisted of individuals from four selected organisations. Organisation One operated in the retail sector of the Australian labour market. The organisation was listed as a top 200 organisation on the Australian Stock Exchange by significance, with over $40 Billion AUD in assets. The organisation employed over 2,500 individuals in their workforce. Thus, the participant sample for this organisation was 45 participants with 22 participants agreeing to engage with the study.

Organisation Two was a large Australian national banking institution. The organisation had an annual income of over $8 Billion AUD, with a workforce that consisted of over 35,000 individuals. Furthermore, the organisation was in the top 200 Australian companies as listed on the Australian Stock Exchange. It was estimated that the participant sample consisted of 73 participants, with 9 participants agreeing to engage with the study.

Organisation Three was a significant private defence industry organisation that operated in Australia as an independent subsidiary of a larger multi-national firm. The firm was listed on Euronext, an European stock exchange. The organisation had a revenue that exceeds $1 Billion AUD and employed over 3,000 individuals in its workforce. The participant sample for this organisation was estimated to consist of 50 individuals with eight participants agreeing to engage with the study.

Organisation Four was a gaming and entertainment organisation. This organisation was listed in the top 200 companies on the Australian Stock Exchange and had a revenue of over $2 Billion AUD, with over 8,000 employees. The participant sample for this organisation consisted of 200 individuals, with 14 participants agreeing to engage with the study.

Nevertheless, out of the anticipated sample population of 368, a response rate of 14% was achieved. From the 53 responses, there were 14 non or un-assessable responses, leaving a response sample of 39 assessable survey questionnaires for analysis.

Table **4** outlines the sample of full-time security employees (FTE) and subsequent response rates

Table 4

Response Rate per Organisation

Organisation	Sample (FTE)	% Response	Responses	Usable Responses
Organisation One	45	48	22	19
Organisation Two	73	12	9	5
Organisation Three	50	16	8	6

Organisation Four	200	7	14	9
TOTAL	368	14	53	39

Organisation One and Three had the highest response rates, with Organisation One having the highest total number of responses. Organisation Four had a response rate of below 10%, indicating a limited survey penetration throughout the security function. Nevertheless, Fowler (2014) suggests that for online surveys, a response rate of 10% is typical for this data collection methodology.

5.2 Response Data

Data was extracted from the completed work measure surveys for each organisation and tabulated for initial analysis. Data was collected from the survey (Figure 4), where various questions were asked about the length of time individuals forecast tasks into the future, their job title and number of staff managed (see Appendix A).

Work Measurement Scale	1 Day – 3 Months	3 Months – 1 Year	1 Year – 2 Years	2 Years – 5 Years	5 Years – 10 Years	10 Years – 20 Years	20+ Years	Not Applicable
How far into the future do you plan your tasks?								
How far into the future do you allocate resources?								
How far into the future is your longest work assignment?								
What is the longest time frame you expect a subordinate to complete work assignments?								
How far into the future do your planning decisions deliver financial return on investments?								
How far into the future are you planning for the development of staff? (Training, Experience)								

Figure 4. Survey Questionnaire Extract

For Table 5.1, tabulated data was aligned across three main scores; the Work Measurement Scale (WMS) score, the Task Complexity Measurement Tool (TCMT) score, and the Job Level score. The Job Level score was a self-selected response of the individuals perceived level of work for validity cross check purposes. The WMS score is an average across all test elements within the scales, with the TCMT score being strongest weighted statement across a series of questions. Following tabulation, data were visualised for further analysis, and a calculation of the spearman rank order correlation between the two measurement tools undertaken.

5.3 Analysis

The following sections articulate the analysis of the raw data for each organisation, including the identified stratum of work for each. Participants responses are plotted according to their assessed surveys, and then simple statistical analysis is undertaken. Following this, each organisation's uncovered roles are ranked according to their identified work level. This analysis is presented below.

5.3.1 Organisation One

Organisation One's security team consisted of 45 individuals. Analysis of the average level of work identified across all three scores indicated individuals to be operating between Stratum Three to Stratum Five. The data suggests one (5%) of participant was operating as a Stratum Five worker, with 13 (68%) assessed as working at Stratum Four, and five (26%) assessed to be working at the level of Stratum Three. Uniquely, all participants identified that they manage staff. This reporting was consistent with Organisation One's participant's self-identified job level and subsequent assessed level of work. Of all the listed job titles, nine used the term *manager*, with only four responses indicating first line or supervisory roles. Figure 5 displays the results from each score, including the average by Job Title, ranked by Job Level score in the first instance. In some instances, Job Title was shared with multiple responses, in which case these have been separated out with a numeric descriptor.

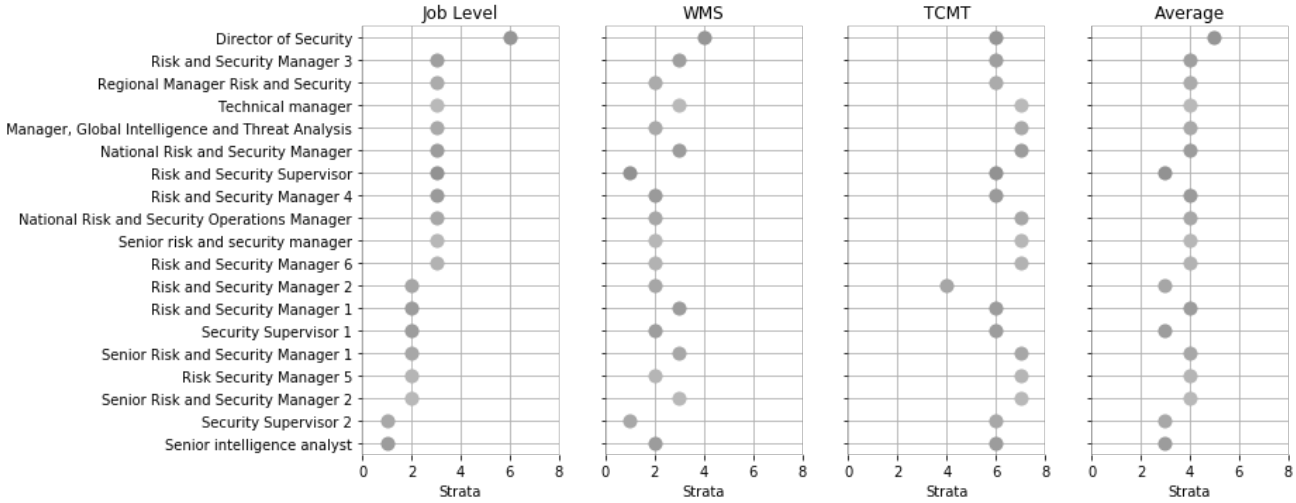

Figure 5. Organisation One Job Level, WMS, TCMT, and Average scores by Job Title

The distribution of scores was plotted (Figure 6), and a high variance between the self-identified Job Level score, WMS score, and TCMT score was discovered. Such variance indicates that the measures are not consistent between each other. It was considered that the distribution of the WMS scores and the self-assessment scores demonstrated less variance than the TCMT distribution, and as such, WMS results were understood to be a more reliable measure of the participants level of work in this instance when compared to the control measure (Ludbey, 2016).

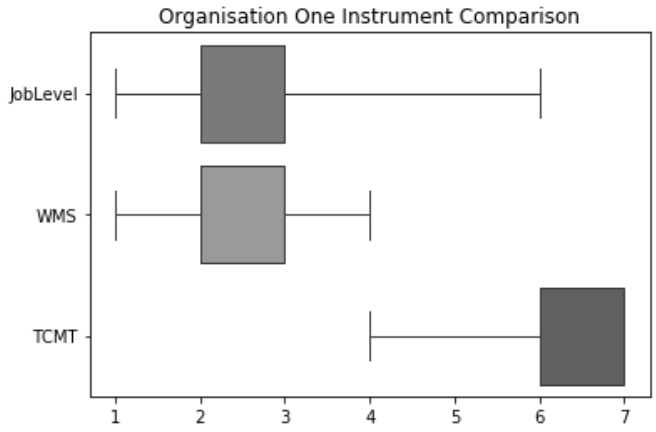

Figure 6. Organisation One Tool Distribution by Stratum

Subsequently using the WMS as the work level indicator, a hierarchy of work was determined for Organisation One, ranging from Stratum Two through to Four (Table 5). Job titles were not repeated in the Table, where multiple entries aligned in the data listed in the data table above.

Table 5

Organisation One Identified Job Titles by Stratum

Stratum of Work	Job Title
Four	Director of Security
Three	National Risk and Security Manager
	Senior Risk and Security Manager
	Risk and Security Manager
	Technical manager
Two	National Risk and Security Operations Manager
	Regional Manager – Risk and Security
	Senior risk and security manager
	Risk and Security Manager
	Security Supervisor
	Manager, Global Intelligence and Threat Analysis
	Senior intelligence analyst
One	Risk and Security Supervisor
	Security Supervisor

5.3.2 Organisation Two

Organisation Two's security team consisted of 73 individuals. Data was tabulated, with individuals being assessed as operating between Stratum Three through to Stratum Five. Consequently, one (20%) participant was assessed as working at Stratum Five, then two (40%) were assessed as working at the level of Stratum Four, and two (40%) were assessed Stratum Three workers. Again, all participants in this organisation identified that they manage staff, which appears consistent with their self-identified job level, job title, and subsequent assessed level of work. Job titles were *management* related, noting that one response did not provide a job title. Figure 7 shows the results from each score, including the average by Job Title, ranked by Job Level score in the first instance.

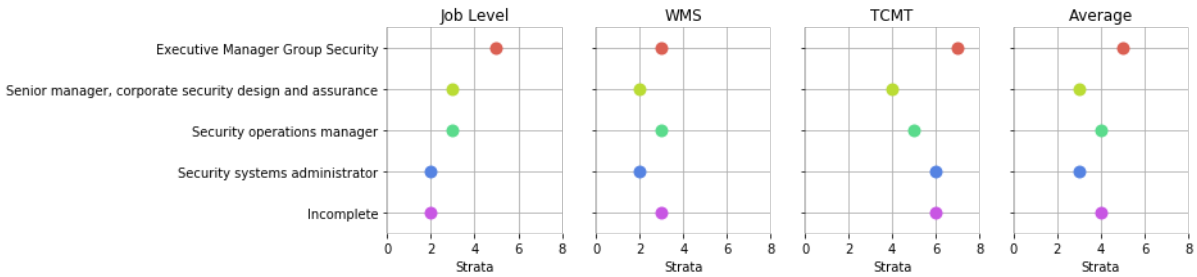

Figure 7. Organisation Two Job Level, WMS, TCMT, and Average scores by Job Title

The distribution of scores was plotted, and a high variance between the self-identified Job Level score, WMS score, and TCMT score was uncovered. Such variance indicates that the measures are not consistent between each other. It was considered in Figure 8 that the distribution of the WMS scores and the self-assessment scores demonstrated less variance than the TCMT distribution, and as such, WMS results were again understood to be a more reliable measure of the participants' level of work in this instance when compared to the control measure.

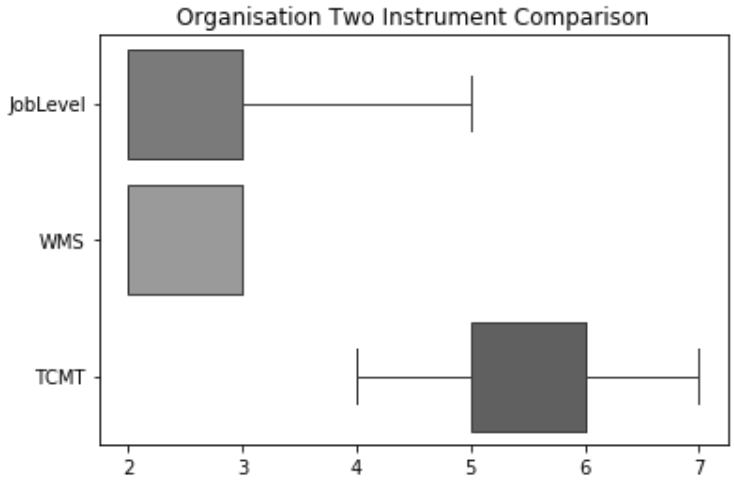

Figure 8. Organisation Two Tool Distribution by Stratum

Subsequently, using the WMS as the measure of work level, the below hierarchy of work was determined for Organisation Two. Security work in organisation two consists of roles in Stratum Two and Stratum Three. Job titles were not repeated where multiple entries aligned in the data.

Table 6

Organisation Two Job Titles by Stratum

Stratum of Work	**Job Title**
Three	Executive Manager Group Security
	Security operations manager
Two	Security systems administrator
	Senior manager, Corporate Security design and assurance

5.3.3 Organisation Three

Organisation Three was a defence industry organisation located in Australia. The organisation security team was estimated to consist of 50 individuals. A total of eight responses were received, where only six were assessable. Figure 9 presents the tabulated data for this organisation, with individuals being assessed as operating between Stratum One through Stratum Six. For this organisation 1 worker (12.5%) was assessed at operating at Stratum Six, followed by 2 (33%) workers being assessed as Stratum Four, 2 (33%) being assessed at Stratum Three, and 1 (12.5%) assessed as Stratum One. All participants except the Stratum One worker in this organisation identified that they manage staff, which appears consistent with their self-identified job level, job title, and subsequent assessed level of work. Job titles were a mix of management related and operational, with three responses not providing a management title. Figure 9 shows the results from each score, including the average by Job Title, ranked by Job Level score in the first instance.

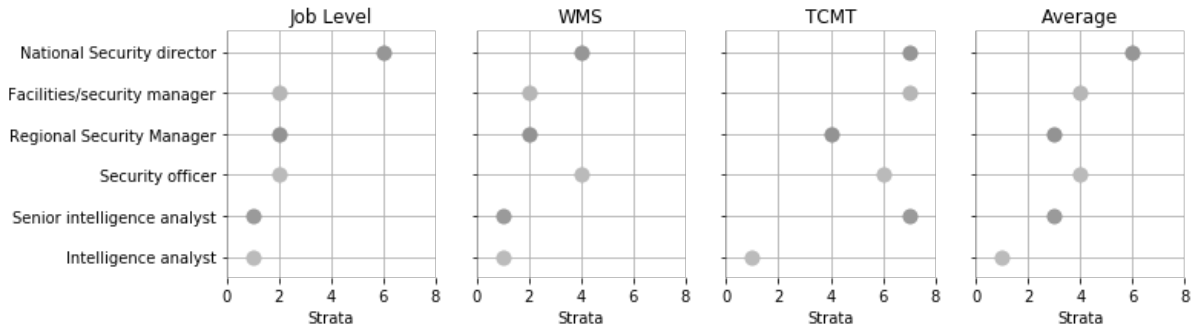

Figure 9. Organisation Three Job Level, WMS, TCMT, and Average scores by Job Title

The distribution of scores was plotted, and a high variance between the self-identified Job Level score, WMS score, and TCMT score was found. Such variance indicates that the measures are not consistent between each other. Figure 10 highlights the distribution of the WMS scores and the self-assessment

scores demonstrated less variance than the TCMT distribution, and as such, WMS results were understood to be a more reliable measure of the participant's level of work in this instance when compared to the control measure.

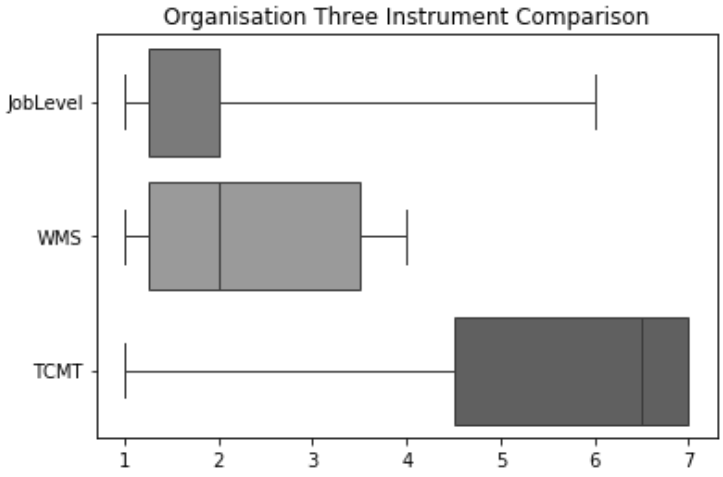

Figure 10. Organisation Three Tool Distribution by Stratum

Subsequently, the below hierarchy of work was determined for this organisation, consisting of roles in Stratum One, Two, and Four. Job titles were not repeated where multiple entries aligned in the data.

Table 7

Organisation Three Job Titles by Stratum

Stratum of Work	**Job Title**
Four	National Security director
	Security officer
Two	Regional Security Manager
	Facilities/security manager
One	Senior intelligence analyst
	Intelligence analyst

5.3.4 Organisation Four

Organisation Four was a gaming and entertainment entity operating in the Australian market. The organisation security team consisted of 200 individuals. 14 responses were received, where only 9 were assessable. Figure 11 shows tabulated data for this organisational sample, with individuals being assessed as operating between Stratum Two through Stratum Four. For this organisation 3 (33%) participants were assessed as working at Stratum Four, 5 (55%) were assessed as Stratum Three, with the remaining worker (11%) assessed as working at Stratum Two. All participants identified that they

manage staff, which appears consistent with their self-identified job level, job title, and subsequent assessed level of work. However, Job titles were a mix of management related and operational task roles, with three responses not providing a management title. Figure 11 shows the results from each score, including the average by Job Title, ranked by Job Level score in the first instance.

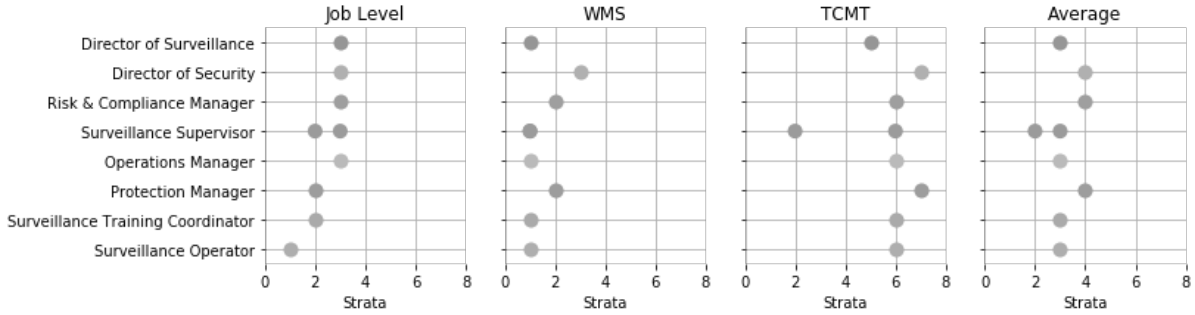

Figure 11. Organisation Four Job Level, WMS, TCMT, and Average Scores by Job Title

Again, the distribution of scores was calculated for each response, with a high variance between the self-identified work level, work measurement scale result, and task complexity measurement tool response recorded (Figure 12). Such variance indicates that the measures are not consistent between each other. As with the previous samples, the WMS tool was considered more appropriate.

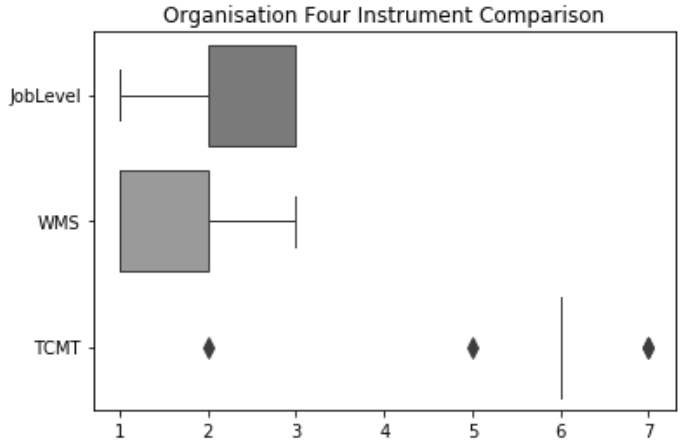

Figure 12. Organisation Four Tool Distribution by Stratum

Subsequently, the below hierarchy of work was determined for Organisation Four, with work consisting of Stratum One, Two, and Three roles. Job titles were not repeated where multiple entries aligned in the data.

Table 8

Organisation Four Job Title by Stratum

Stratum of Work	**Job Title**
Three	Director of Security
Two	Protection Manager
	Risk & Compliance Manager
One	Director of Surveillance
	Surveillance Training Coordinator
	Surveillance Operator
	Surveillance Supervisor
	Security Supervisor
	Operations Manager

5.3.5 Organisational Spread

A violin plot was provided for each organisation (Figure 13). Such a plot visualises the probability density of each strata within the identified organisation security work structure by plotting the distribution of the data (Hintze & Nelson, 1998). The plot used the WMS score for each respondent in each organisation to visualise the work structure and reporting hierarchy. Subsequently, in these distributions, it can be seen that Organisation One appears to be weighted in the middle tiers of their organisation strata, where Organisation Two is weighted towards the higher strata of work. Organisation Three is seen to have a spread reporting hierarchy, and Organisation Four has the majority of employees in the Stratum One category as would be expected in a traditional hierarchical work structure (Robbins & Judge, 2012).

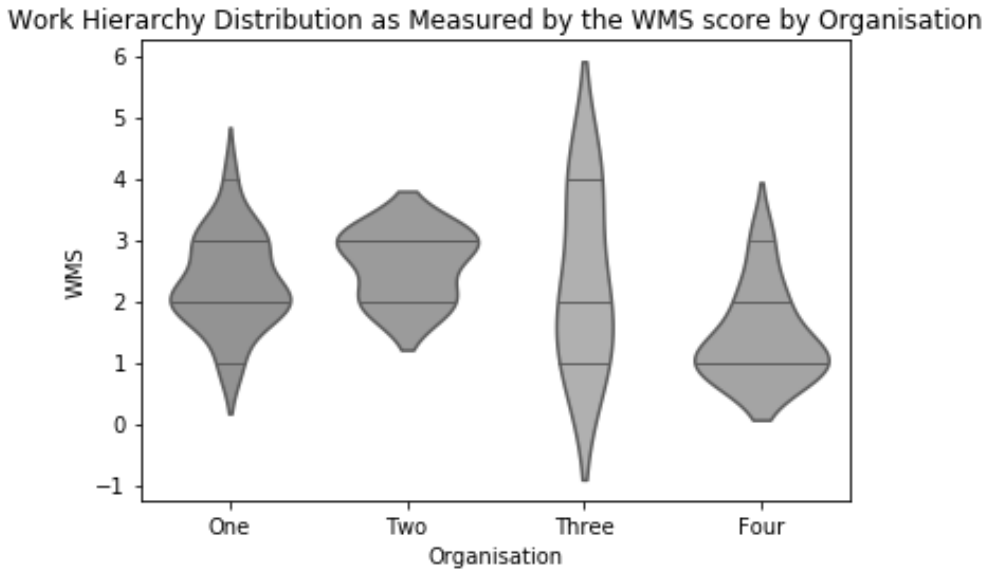

Figure 13. Uncovered Work Hierarchy Distribution

5.4 Reliability and Validity

The reliability and validity section outline a cross-organisation comparative test in Section 5.4.1 using the Kruskal-Wallis measure. Then, the section considers a Spearman Rank Order correlation for each test-pair in Section 5.4.2. These statistical tests provide insight into the reliability and validity of the findings, and thus their investigative power in the study phase.

5.4.1 Cross-organisation comparison

In consideration of reliability and validity of these results, a cross-organisation comparative test was undertaken using the Kruskal-Wallis non-parametric measure. A statistically significant result on any of the measures indicates that the sample from each organisation are part of the same occupational population (Field, 2013). Such an outcome is important, as it suggests that the data collected is of 'typical' Corporate Security practitioners. The data were analysed (Table 9), with the Work Measurement Scale demonstrating significance (p=0.05596, < .10). However, both the TCMCT (p=0.40287, < .10) and self-assessment (p=0.47459, < .10) results were not significant.

Table 9

Kruskal-Wallis test results per measure

Test per Measure	**Score**
Kruskal-Wallis - WMS	P=0.05597, < .10 - Significant
Kruskal-Wallis - TCMT	P=0.40287, < .10 – Not significant
Kruskal-Wallis Self	P=0.47459, < .10 – Not significant

Consequently, the WMS result is considered to be the most valid statistical result, and as such was considered the primary measure of work for Phase One of the study. Such a finding is consistent with the analysis and distribution plots conducted in Section 2 for each individual organisation, aligning with previous studies using this tool (Ludbey, 2016; Ludbey et al., 2017). Furthermore, it was noted that this measure of work was relatively weak in its predictive power. For example, as Stamp (1981), Jaques (1996), Ivanov (2006), and later Clement and Clement (2013) discuss, it can be difficult to identify an individual stratum of work without extensive interviews as the analysis process can be subjective in nature.

Nevertheless, such a finding suggests that the four organisational samples, when measured on the WMS, come from the same occupational population. Such a finding provided some evidence for extrapolation to a 'typical' result; that is, a typical Corporate Security hierarchy. Further investigation into the applicability of the TCMT tool in future research should be conducted, as it appeared to be an unreliable measure across each organisation and over all data collected.

5.4.2 Spearman Rank Order Correlation Test

A Spearman Rank Order Correlation Test was conducted on each test-pair per organisation, and between each test-pair for the combined organisation data set. Such tests were conducted to understand the correlation between each measure, those being the Work Measurement Scale, the Task-Complexity Measurement Tool, and the Self-Assessment. The Average score was not tested as this was derived from an average of the three measures above, meaning that it would always correlate.

Table **10** tabulates the outcomes of these tests, which highlights that the correlation between measures for Organisation One and Two did not occur within a statistically significant range; however, the WMS and Self-Assessment pair was statistically valid (WMS:Self Assess - R=0.9037, P=0.01347) for Organisation Three, while the other two pairs were not (WMS:TCMT - R =0.254, P=0.62719; TCMT:Self Assess - R=0.3607, P=0.48241).

Table 10

Spearman Rank Order Correlation per Test-Pair per Organisation

Organisation	**Spearman Rank Order – WMS and TCMT**	**Spearman Rank Order – WMS and Self Assess**	**Spearman Rank Order – TCMT and Self Assess**
Organisation One	R=0.21321, P=0.38082, Not Significant.	R=0.23323, P=0.33658, Not Significant.	R=0.1958, P=0.42176, Not Significant.

Organisation Two	R=0.44426, P=0.45355, Not Significant.	R=0.30429, P=0.61863, Not Significant.	R=0.10815, P=0.86257, Not Significant.
Organisation Three	R = 0.254, P=0.62719, Not Significant.	**R=0.9037,** **P=0.01347, Significant.**	R=0.3607, P=0.48241, Not Significant.
Organisation Four	**R=0.72923,** **P=0.02579, Significant.**	R=0.24499, P=0.52521, Not Significant.	R =0.04103, P=0.91653, Not Significant.
All Organisations	**R=0.34445,** **P=0.03177, Significant.**	**R=0.36426,** **P=0.02262, Significant.**	R=0.20694, P=0.20621, Not Significant.

The WMS and TCMT pair for Organisation Four was statistically valid (WMS:TCMT - R=0.72923, P=0.02579), while the other two pairs were statistically insignificant (WMS:Self Assess - R=0.24499, P=0.52521; TCMT:Self Assess - R =0.04103, P=0.91653). Finally, taking an overview of all the data collected between organisations, the WMS and TCMT pair was statistically valid, as was the WMS and self-assessment measure (WMS:TCMT - R=0.34445, P=0.03177;WMS: Self Assess - R=0.36426, P=0.02262). The TCMT and self-assessment pair was not statistically significant across all organisations (TCMT:Self Assess - R =0.04103, P=0.91653).

These findings may suggest that the three points of measure are not aligned and do not measure the same construct. Alternatively, due to the relatively low sample size from each population, it is also considered that statistical correlation may be difficult to achieve (Field, 2013). For example, Witte and Witte (2017, p. 119) describe small sample sizes can impact the capacity of calculations such as the Spearman Rank Order due to the impact of outliers. Nonetheless, in reference to Laerd Statistcs (2013) the correlation between the WMS and TCMT, and the WMS and Self-Assessment across all four organisations provides some confidence that the measures have a monotonic relationship, that is, where a statistically significant correlation has been found, each measure has a linear relationship. Such findings suggest that the instruments in these cases are measuring the same construct (Laerd Statistcs, 2013).

5.5 Phase One Interpretation

Phase One sought to respond to the study's first sub-research question by investigating the stratum of security practitioners within Australian Corporate Security hierarchies. The sub-research question was: *What is the stratum of security practitioners in the corporate organisation context?*

A number of themes emerged from the data analysis to respond to the Research Question. These themes align with the socio-organisational literature, specifically the articulation of corporate roles

and hierarchies (Clement, 2015; Jaques, 1996). Phase One of the study found that security work is hierarchical and stratified generally within the predictions of the management theory espoused by Jaques (1996). This theory holds that organisational business units, including the security function, have a defined leadership, with levels of work between Stratum One through Five. Roles beyond this Stratum Five ceiling are considered executive positions that are highly generalist in nature. Nonetheless, it must be acknowledged that some Phase One findings indicate that modern organisational structure could impact this understanding of work, and subsequently the findings.

The Phase findings provide an insight into security work within Australian organisations, providing some evidence towards an understanding of a typical Corporate Security function. While the results are not statistically substantial enough to support a rigorous and holistic model of security work, they provide evidence to refute some claims and verify others made by the security literature about organisational structure and the security occupational stratum (Bamfield, 2014). Such refuted claims include the existence of an executive security stratum, and the subsequent importance of the security function as a whole. Furthermore, the findings tend to be in agreement with Ludbey et al. (2017), where security is a tactical technostructure unit who does not directly contribute to profit making activities but shapes the operating environment by reducing uncertainty and risk (Mintzberg, 1980; Robbins & Judge, 2012). These themes are further discussed in the following sections.

5.5.1 The Corporate Security Stratum of Work

The Corporate Security stratum of work was uncovered in the phase findings. These included roles located in Stratum One, Two, Three, and Four, which are classified as operational and tactical role seatings. Each strata is presented below, and includes discussion about the identified taskings for each role, as well as differences between the participatory organisations.

5.5.2 Stratum One

Organisation One participants at this stratum indicated that their most common task was ‘first aid’ and ‘signing off on reports’. Organisation Three participants were similar, with work consisting of ‘reports’ and ‘daily reporting to clients.’ Finally, Organisation Four participants conducted work such as ‘staff management’, ‘training staff’, ‘monitor CCTV’, ‘ensure integrity of organisation’, ‘evaluate potential threats’, and ‘managing incidents.’ It is suggested that ‘staff management’ is an outlier, as such tasks generally are conducted at higher strata of work.

Nevertheless, Organisation Four had a series of hierarchical roles, which were all captured in the Stratum One category of work. Specifically, the roles of Director of Surveillance, Operations Manager, Surveillance Supervisor and Surveillance Operator were all captured in this stratum of work.

Such a finding could suggest that Organisation Four is heavily compressed, at least in the surveillance operational unit (Ivanov, 2011). While the literature states that a compressed organisation is one where several hierarchical roles are assigned tasks within the same time span of discretion as their direct reports, leading to conflict and inefficiency, context may explain why such compression exists.

Alternatively, Brooks and Smith (2012) highlight that security can only be defined through operational context, which indicates that the identified stratum of work for this organisation could also be aligned to the specific circumstances of its operational requirements (Johns, 2006). Organisation Four's security team is focused on the monitoring of gaming tables and other such activities in alignment with the legislative and regulatory requirements of the states that it operates within. Therefore, perhaps due to the operational focus of surveillance security activity, managerial staff in this organisation are required to remain focussed on the day to day activities of the organisation and as such; do not operate at the higher strata (Dadashi, Stedmon, & Pridmore, 2013; Donald, 2010). If such an outcome were accepted, the requirement for so many hierarchical positions within this stratum of work should not be required under a more efficient work structure.

Table 11

Uncovered Stratum One Roles

Organisation One	Organisation Two	Organisation Three	Organisation Four
Risk and Security Supervisor, Security Supervisor	NA	Senior Intelligence Analyst, Intelligence Analyst	Director of Surveillance, Surveillance Training Coordinator, Surveillance Operator, Surveillance Supervisor, Security Supervisor, Operations Manager

Nevertheless, the findings at this stratum somewhat align to the broader security literature, where front line workers and supervisors make up the security workforce on the ground (Nalla & Wakefield, 2014; Sennewald, 2011). Notwithstanding the severe misalignment of more senior roles found in Organisation Four, the positions identified in each of the organisations spread across several distinct security operations, such as intelligence, general security officers, and surveillance operators. This spread of security operations outlines that the operational strata of security works carry across several sub-disciplines and is not limited to one particular segment of the security community (Brooks, 2013; Brooks & Corkill, 2014).

5.5.3 Stratum Two

When considering those participants who aligned to Stratum Two roles, several key work functions emerged. For example, Organisation One work consisted of 'threat analysis', 'project management', 'customer relations', 'asset and brand protection', 'dealing with public liability incidents', and 'Create a safety environment and culture while making sure I have a good coordinated emergency response team'. Such roles indicate higher order thinking and longer-term achievements, for example working toward a coordinated emergency response team is clearly a supervisory role in alignment with Jaques (1996) due to its focus on immediate team-based goals. Further, Organisation Two roles consisted of 'managing projects' and 'security install projects', which align with the expected shorter-term risk mitigation strategy implementation. Organisation Three roles consisted of 'reports and meetings' and 'security compliance and process'. Finally, Organisation Four roles consisted of 'analyse data'.

While these tasks comfortably align with Stratum Two roles, the individual corresponding job titles suggest that each organisation has created senior roles to carry out tasks that are better suited to

those closer to the 'coal face' of organisational operations. Such a workforce structure is likely to lead to instability in operations and inefficiency in carrying out complex risk mitigation strategies (Ivanov, 2006). In consideration of the evidence collected in this phase, these organisations appear to have general management staff creating and then implementing security strategy, without a delegation layer in between to handle operations in discrete units. While this may be seen as efficient from a particular point of view (less staff), what is more likely to occur is a lack of detailed attention to each component part of the overall security strategy (Brooks & Smith, 2012).

Table 12

Uncovered Stratum Two Roles

Organisation One	**Organisation Two**	**Organisation Three**	**Organisation Four**
National Risk and Security Operations Manager, Regional Manager – Risk and Security, Senior Risk and Security Manager, Risk and Security Manager, Security Supervisor, Manager -Global Intelligence and Threat Analysis, Senior Intelligence Analyst	Security Systems Administrator, Senior Manager - Corporate Security Design and Assurance	Regional Security Manager, Facilities/Security Manager	Protection Manager

Importantly, in an ideal work hierarchy, managerial oversight of a series of security risk mitigation measures should be carried out in a Stratum Three or Four role (Jaques, 1996). Where occupational titles such as 'National Risk and Security Operations Manager' and 'Regional Manager – Risk and Security' and 'Manager – Global Intelligence and Threat Analysis' have been identified as Stratum Two, it would be expected that these roles would be higher ranking due to their apparent senior positioning. Either these roles are compressed to the point where they are severely underutilised due to the restrictions of their operating time span or have been allocated occupational position titles that do not align with their expected roles function. Such a misalignment in occupational title and actual organisational seniority may be the more likely outcome if organisations do not understand where security fits within the organisation structure (Fayol, 1916/1949; Gill & Howell, 2012; McGee, 2006).

5.5.4 Stratum Three

Stratum Three work in Organisation One consisted of 'overseeing operational risk within [the] organisation', 'training / consultation', 'responding to requests', 'security and public liability related matters', and 'managing the risk and security for the organisation in a specific location'. Organisation Two work consisted of 'collation of physical and operational risk assessments', and 'day to day security operations management'. Organisation Four work consisted of 'managing change'. Such roles are articulated in Clement and Clement (2013), quite closely aligning these responses to Stratum Three work.

Roles such as 'Director of Security' should be located further up the stratum according to the literature (Bamfield, 2014; Sennewald, 2011); however, the findings suggest that perhaps such a role in this case it not operating at that higher level, or the security function is compressed as seen in previous strata. If the roles are not operating at a higher level of work, conceivably the security business unit is not a mature function and as such, is not wholly embedded within the organisation (Burnstein, 1978). Consequently, the role fulfilled by the security business unit could also be responsible for this lower stratum placement. For example, a comprehensive and mature security function incorporating all aspects of security would be expected to have a more robust employment hierarchy and operate at higher strata of work (Interim Security Professional's Taskforce, 2008), whereas a targeted function such as a loss prevention team would operate around Stratum Three of work at its peak (Barefoot & Maxwell, 1987; Jaques, 1996).

Nevertheless, security works at this stratum seem to consist of coordination and management of security risk and threat assessments, and other such activities, which is consistent with the security literature (Brooks & Corkill, 2014). Notwithstanding the occupational title misalignment, work at this level seemed consistent with Jaques (1996) predictions, as threat and risk assessments for example require longer term thinking and the capacity to draw reasonable conclusions from a variety of internal and external sources (Ludbey & Brooks, 2017; Talbot & Jakeman, 2009).

Table 13

Uncovered Stratum Three Roles

Organisation One	**Organisation Two**	**Organisation Three**	**Organisation Four**
National Risk and Security Manager, Senior Risk and Security Manager, Technical Manager	Executive Manager Group Security, Security Operations Manager	NA	Director of Security

5.5.5 Stratum Four

Organisation One work consisted of 'develop, deliver strategy', and Organisation Three work consisted of 'representation and policy'. Such roles partially align with what Clement and Clement (2013) calls a 'Functional Manager' at Stratum Four who integrates discrete activities into a single function, and manages people, processes and resources.

Interestingly, the roles found in the participant sample of Phase One consisted of Director of Security roles. This role alignment suggests that the security occupation within the four organisations samples meets a ceiling at the Stratum Four level. Such findings are consistent with Ludbey and Brooks (2017) and Ludbey et al. (2017) who found that the highest level of security works was at the Stratum Five level. While the roles uncovered at this stratum of work appear to be executive level roles based on the job title, further investigation is required to determine where these roles fit within the broader complexity of the organisation. They have been assessed as middle management based on their time-span of discretion; however, the misalignment of the role title and role assessment could be the result of several factors.

Table 14

Uncovered Stratum Four Roles

Organisation One	**Organisation Two**	**Organisation Three**	**Organisation Four**
Director of Security	NA	National Security Director	NA

5.6 Limiting Factors for Corporate Security

As articulated, the Phase findings uncovered a stratum of work stretching across Stratum One, Two, Three, and Four for Corporate Security practitioners. Subsequently, consideration was given to the reasons why practitioners, particularly those with executive titles, were note located further up the work strata as would be expected for such roles (Bayuk, 2010; Jaques, 1996). These considerations included the role of uncertainty, occupational success, organisational complexity, organisational misalignment, and organisational compression.

5.6.1 Managing Uncertainty

All four organisations had individuals present in both the operational and tactical segments of the work strata. Such a spread of roles in all assessed organisations suggests that the Corporate Security groups are seen to be important and valued to some extent by the organisation (Heath, 1981). As

discussed by Ludbey et al. (2017) the value derived by the organisation from the security function is due to its technostructure function. Further evidence of this finding is found in this phase, with role descriptions suggesting security practitioners are reducing uncertainty to the organisations operations by understanding their threat and risk exposure, as opposed to influencing profit making activities. Such a specialisation in managing security uncertainty and risk however, could lead to a progression ceiling, as higher order organisation positions require more generalist problem solving capabilities (Maitland & Sammartino, 2014).

According to Jaques (1996), managing uncertainty is a key element in an individuals' capability to conduct work at higher strata, as it allows for higher-order thinking (Jaques, 2002). As Mintzberg (1980) describes, technostructure functions 'advise' the organisation, and rather than produce profit, aid organisation operations in other ways (Jo, 2018). Such an articulation closely aligns with the findings, as no role descriptors within the first phase identified profit-making activities, but instead suggested the implementation of strategies to reduce harm.

5.6.2 Occupational Success

An additional conjecture for the identified literature misalignment is the role played by Corporate Security's overall occupational success. As considered by Strauss (1975/2001), highly specialised work functions tend to have fewer hierarchical progression opportunities within organisations. Holland et al. (2012, pp. 122-134) agrees, which due to the focussed nature of some of the identified senior security roles (i.e. "Overseeing operational risk and security within [the] organisation" – National Risk and Security Manager), provides an explanation for the Stratum Four occupational peak.

Class plays a significant role in occupational progression within organisations as well. Freidman et al. (2015) argue that those who come from lower classes (as in, birth right, financial security, education etc.) do not often progress to the peak of occupational work hierarchies. McGregor (1997) highlights that in Australian society, education is the most influential class mobility factor, which is supported by Dubow, Boxer, and Huesmann (2009) who suggest that an individuals' parent's education level can have long standing impacts on career success. The findings from Phase One do not provide enough information about these traditional class identifiers to postulate the influence of these factors; however, there could be a link between these class components and the corresponding peak of the security work hierarchy.

5.6.3 Organisational Misalignment

According to Ivanov (2015b), the CEO of an organisation is the only individual within an organisational hierarchy that has a full picture of the strategic worldview of the enterprise. Subsequently, each hierarchical layer beneath this position has an ever-restricted version of this organisational picture

because their understanding of the organisation is defined specifically by their role, responsibilities and reporting relationships. The inherent delegation of responsibility and tasks down the hierarchy inevitably reduces the operating picture of each role due to the inherent increase in specialisation (Mumford et al., 2007). Furthermore, Ivanov (2015b), further suggests that managers can realistically only implement their delegated responsibility; true innovation can only come from the highest reaches of the organisation where a more holistic understandings of the operating environment occur.

Consequently, it is postulated that those peak security roles that are not operating at the strata of work suggested by the security literature could be due to the executive staff not delegating or defining the appropriate responsibilities for these positions. It would follow that an executive team hiring for a Director of Security, but whom did not create the remit for a fully comprehensive and integrated security function (such as those described in an idealistic sense by Cubbage and Brooks (2013) or Talbot and Jakeman (2009) when discussing enterprise risk management transformation) would result in reduced responsibility, authority, and finally, stratum of work. The consequence of such a hire would be seen through each subsequent subordinate role, as these occupational placements would be defined by the security Director in the first instance—a reduced remit in the first instance necessarily leads to a reduced delegated authority down the chain.

This study did not explore this investigation further, as it would benefit from a broader and deeper investigation in further research. The collection of data from security practitioners only in this research inherently restricted the capacity of the researcher to further explore this authority-delegation nexus further.

5.6.4 Organisational Complexity

Alternatively, there is some evidence to suggest that non-multinational organisations operate at a lower maximum stratum of work than Stratum Seven (Jaques, 1996). McMorland (2005) outlines CEO roles that operate at Stratum Four or Five, with subsequently less hierarchical layers in their managed organisation than those that operate at higher order strata. Ivanov (2015a) supports this view, suggesting that Stratum Seven organisations are generally multinational, and stand-alone organisations operate at a peak of Stratum Five. Such findings could influence the seating of senior security occupational roles as found in Phase One; if the participant organisations top out a lower stratum than suggested by Jaques (1996) then all roles beneath the CEO would be of lower order strata as well.

In contrast, it is suggested by Barkema, Baum, and Mannix (2002) that work complexity is increasing due to the implications of globalisation and information technology on typical occupational roles. Subsequently, even if maximum role alignment is found at a lower stratum in modern organisations,

the roles being fulfilled are likely to be more complex than those measured by Jaques (1986). While this increase in complexity may not influence individual roles time-span of discretion, which is the primary measure used to map out the identified work strata, it is suggested that complexity will have a non-negligible influence on the results. As articulated by Le Grand and Tahlin (2013), complexity plays a substantial role in determining hierarchical position (Bazerman & Moore, 2009).

Nevertheless, it is noted that three of the four participant organisations were multinational, in particular Organisation One, Two and Three. Admittedly, without data collection occurring across the entire organisation non-specific to the security function, it is difficult to postulate the true highest level of work in the organisation, and as such, difficult to surmise the appropriate occupational strata / participant level of work fit. Therefore, it is suggested that future research explore this hypothesis in detail.

5.6.5 Organisational Compression

On the other hand, Ivanov (2015a) suggests that most work occurring in modern organisations are compressed into the lower order strata, with severely limited time-spans and the requirement for tight deadlines at the sacrifice of considered decision making (Ivanov, 2015a). It could be argued that the increasing complexity of globalisation, alongside dramatic shifts in information technology have led to a more operational focus along the entire organisation hierarchy (Barkema et al., 2002; Stichweh, 2008). Where in the past, organisations were more clearly defined between strategic and non-strategic decision making—and this decision making was over longer periods of time, today strategic decision making is more common for shorter time periods due to the rapid changes in global market conditions (Barkema et al., 2002; Ries, 2011). Such fundamental shifts in organisation decision-making could have substantial effect on the measured time span of discretion of the participants selected in Phase One.

Nevertheless, Clement (2015), and Boal and Whitehead (1992) suggests that time span can be further compressed when an individual or groups of individuals are under pressure or stress in the workplace. For example, during war fighting conditions, soldiers and decision makers can drop two full strata of work in their operational time-span of discretion due to stress and immediacy of the events unfolding. In these cases, while the time span decreases, the complexity of the role is not; resulting in individuals not considering second and third order consequences of their decision-making.

5.7 Focus Group Questionnaire

Throughout the interpretation of the Phase One results, it has been identified that the security work hierarchy is in somewhat of a disagreement with the security literature. By unpacking the data within the literature frame, several theoretical explanations for the uncovered misalignment are introduced.

It is important to clarify these explanations through targeted data collection. Therefore, the study's Phase Two asked: *To what extent does the Corporate Security function permeate throughout organisations?*

Therefore, a targeted series of questions were developed for the Phase Two data collection process. The investigation considered organisation compression, and occupational success in the second phase. In review of organisation compression, queries about individual roles and their inherent complexity were considered. Such questions uncover the extent to which roles are operationally focussed, stressful, or overly complex from a literature perspective. Moreover, to broaden the understanding of the security occupation from a sociological and class perspective, questions about education, career progression, and previous work experience were developed. As outlined by Heslin (2005) occupational success depends on a variety of these factors and could significant influence the strength of progression ceilings.

The developed questionnaire is seen overleaf:

Table 15

Phase Two Questionnaire and Question Purpose

No.		**Question**	**Purpose**
1	Occupational Success	Could you explain how you started work in the security industry?	A broad background question will provide some understanding of sociological influences on work and career choices.
2		Could you explain your work experience?	Understand Experiential requirements for current role, as well as gather broader sociological information about possible class background.
3		Can you talk about the duties you undertake in your role?	Understand role makeup, impact, and purpose.
4		Could you elaborate on the value security brings to your organisation?	An understanding of the perceived value that security brings to the organisation could indicate the alignment of security to profit, and thus, success.
5	Organisation Complexity	How complicated is your work?	An understanding of perceived complexity with each strata-group could provide an indication of compression.
6		Could you explain the unique stresses that come with a security role?	Explore work stress along the stratum; compression can be caused by stress.
7		When you make decisions and start a task or project, is there a lot of uncertainty that you have to deal with?	It would be considered that more uncertainty would correlate to more complexity.
8		Is the security environment changing faster now than it has been in the past?	It is expected that such a question would allow the participants to elaborate on factors that indicate complexity. Increased uncertainty and change would be indicators of compression.
9	Progression Ceiling	Could you explain what career pathways are open to you with your security experience?	Identify stratum of potential work with security experience; do the participants think that a security career can be particularly limiting?
10		How would you 'move up' in the organisation with a security background?	Understand career progression requirements within the organisation from a security specialisation into more generalist roles.
11		Do you think there is a point where security managers need to leave security to progress into more senior roles in an organisation?	Understand if there is a perceived ceiling of progression for security staff.

5.8 Conclusion

By contextualising the research Phase One findings within the literature—where society is stratified along a class and occupational hierarchy in pursuit of capitalistic goals, it is clear that security is a relatively important career path (Cubbage & Brooks, 2013). Each organisation considered in the

research had a significant variety of security roles, ranging from executive job titles through middle management and operational roles. Such a spread of occupational positions is indicative of a work force that is known by the organisation to be an important contributor to business operations (Robbins & Judge, 2012). Such a spread of security roles suggests that, as articulated by Heath (1981), Corporate Security has been somewhat legitimised in Australian organisations through acknowledged achievements and demonstration of worth.

What is unclear from the findings in Phase One however, is the significance of the occupations social power. Due to the relatively low strata ranking of even the most senior roles, it could be that security roles are not considered as socially important as peer-equivalent roles as other functions such as finance. Such considerations are investigated further in Phase Two; however, this indication is interesting as it suggests that security practitioners are excluded from the professions by social standing (Selander, 1990; Wakefield, 2014).

Nevertheless, a clear stratum of security work has been identified, with non-trivial occupational roles discovered within four significant Australian organisations. Four explanations for the identified stratum are provided, including organisation compression, organisation complexity, organisation misalignment, or occupational success. These four suppositions are explored in the following Phase.

CHAPTER SIX

PHASE TWO INTERVIEWS AND FOCUS GROUPS

6.0 Introduction

The Chapter presented the outcomes from Phase Two, which included semi-structured interviews with organisation executives, and focus groups with executive teams and lower strata occupation groups. The interviews and focus groups were conducted across three organisations, with a questionnaire developed in Phase One. Drawing from the findings uncovered in Phase One and enhanced through the discourse of the focus groups and interviews, Phase Two provided a deeper understanding of Corporate Security's function within each of the participating organisations. Such an understanding facilitates a more accurate articulation of security careers, roles, and possible progression ceilings for domain participants.

Subsequently, participants identified numerous factors that may influence their individual security career progression, as well their perception of others in the industry's career progression. Participants also identified the way in which the Corporate Security function operates within the participant organisations, including their perceived value in providing support to organisational activities. The Chapter findings are braced by reliability and validity techniques, including the provision of rich text quotes and supporting transcripts (Qu & Dumay, 2011). Consequently, this Chapter presented the interview and focus group participants, their interview data including key quotes and the themes identified in the formal analysis coding processes (see Chapter 3).

6.1 Participants

Participants included a purposively selected representative Corporate Security sample from three of the four participating organisations in Phase One. After completion of Phase One, individuals were asked to further participate in the upcoming semi-structured interviews and focus groups. Initially semi-structured interviews were conducted with senior executive staff members who were unavailable to participate in the focus groups, followed by focus group interviews with the remaining executive cohort. Upon conclusion of this initial round of interviews and focus groups, executives nominated appropriate subordinate staff members to be selected for participation in the next round of focus group interviews. Such an approach is consistent with a snowball sampling methodology (Cohen, Manion, & Morrison, 2007), enabling an approach to the various levels (strata) of work within each organisation to collect the data.

6.2 Participant Sample

The participant sample consisted of 15 individuals across seven interview groups from three of the four organisations selected for Phase One. The sample selection included individuals (N=1) of senior executives for semi-structured Interviews and N=14 of executive and operational strata participants to undertake the focus group component. Semi-structured interviews were conducted in person. Then, focus groups were conducted in person where possible; however, in some instance's teleconferences were undertaken. This mixed approach to the data collection was accepted to ensure high levels of rich engagement across the organisations; facilitating more detailed data collection than would have been otherwise possible.

In the data collection, participants were coded (Individual Reference Code) as depicted below in Figure 14.

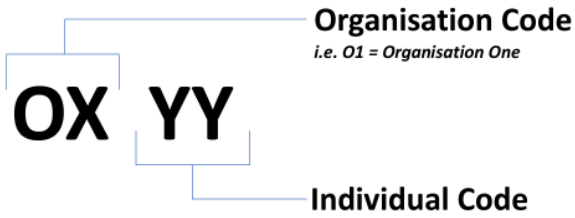

Figure 14. Individual Reference Code

6.2.1 Semi Structured Interviews

As articulated, where participants could not attend focus groups, semi-structured interviews were held. Organisation Two required an interview at the executive strata and is discussed below.

6.2.2 Interview One - Executive

Interview One was undertaken in a conference room at Organisation Two's head office. Table 16 presents the participants' professional information including their reference code, occupation title, level of education and career experience.

Table 16

Interview One Participant

Individual Reference	Title	Qualifications or Certifications	Career
O2PM	Chief Security Officer	Bachelor of Business, Management, and Accountancy Master of Science (Security and Risk Management)	Police Investigations Corporate Security

6.2.3 Focus Groups

Focus groups were conducted across all three organisations at both the executive and operational strata. The participant individual reference code is derived in the same way as articulated in Section 6.2.1

6.2.4 Focus Group One - Operations

Focus Group One was undertaken in a conference room at Organisation One's head office. Table 17 presents participants professional information including their reference code, occupation title, their level of education and career experience.

Table 17

Focus Group One Participants

Individual Reference	Title	Qualifications or Certifications	Career
O1C	Security Site Manager	Unknown	Security operations
O1BG	Risk and Security Manager	Adv. Diploma in Hotel Management Diploma in Management Cert. IV in Training and Assessment Cert. IV in Risk Management Cert. III Technical Security	Security operations Event security Security technology Security management

6.2.5 Focus Group Two – Executive

Focus Group Two was undertaken over teleconference.

Table **18** presents participants from Organisation One's professional information including their reference code, occupation title, their level of education and career experience.

Table 18

Focus Group Two Participants

Individual Reference	Title	Qualifications or Certifications	Career
O1AW	National Risk and Security Manager	Bachelor of Commerce	Retail Management

			Corporate Security
O1NH	National Risk and Security Operations Manager	Diploma Security and Risk Management Diploma Government Investigation Cert. IV Workplace Training and Assessment Cert. IV Project Management Cert. III Investigative Services	Police Investigations Corporate Security
O1LT	Manager, Global Intelligence and Threat Analysis	Bachelor of Arts (French and Sociology) Bachelor of Arts (Global Politics and International Relations) with First Class Honours	Strategic Advisory Corporate Security Intelligence

6.2.6 Focus Group Three – Operations

Focus Group Three was undertaken in a conference room at Organisation Two's head office.

Table **19** presents participants professional information including their reference code, occupation title, their level of education and career experience.

Table 19

Focus Group Three Participants

Individual Reference	Title	Qualifications or Certifications	Career
O2SH	Senior Manager, Travel Security, Intelligence, and Social Media	Masters of Research, (Counterterrorism) Masters of International Security, Terrorism, and Counterterrorism Operations Bachelor's Degree, Criminology Diploma Risk Management	Police Corporate Security
O2MR	Senior Manager Corporate Security, Design	Unknown	Building Control Systems / Home Automation Security System Design
O2LS	Manager Event Security	High School	Security Operations Event security

6.2.7 Focus Group Four – Executive

Focus Group Four was undertaken in a conference room at Organisation Two's head office. Table 20 presents participants professional information including their reference code, occupation title, their level of education and career experience.

Table 20

Focus Group Five Participants

Individual Reference	Title	Qualifications or Certifications	Career
O2PG	Executive Manager, Security	Unknown	Risk Corporate Security
O2SM	Executive Manager, Protective Security	Master of Science (Security and Risk Management) Master of Business Administration Master of Science (Health, Safety, and Risk Management)	Army Close Protection Corporate Security

6.2.8 Focus Group Five – Operations

Focus Group Five was undertaken over teleconference with participants from Organisation Three. Table 21 presents participants professional information including their reference code, occupation title, their level of education and career experience.

Table 21

Focus Group Five Participants

Individual Reference	Title	Qualifications or Certifications	Career
O4SM	Operations Manager	Unknown	Army Security Operations
O4BB	Surveillance Duty Manager	Bachelor of Accounting	Entertainment and Gaming Security Operations

6.2.9 Focus Group Six – Executive

Focus Group Six was undertaken in a conference room at the researcher's office. Table 22 presents the participants from Organisation Three's professional information including their reference code, occupation title, their level of education and career experience.

Table 22

Focus Group Six Participants

Individual Reference	Title	Qualifications or Certifications	Career
O4CC	Director of Surveillance	Bachelor of Counterterrorism, Intelligence, and Security Cert. III Investigations	Security Operations Security Management
O4DM	Risk and Compliance Manager	Cert IV Security Risk Management	Security Operations Security Management

6.2.10 Questionnaire

Each focus group and semi-structured interview participant was asked a series of questions developed in Phase One. Each question was asked in order, with follow up questions to clarify or expand responses provided by the participants. The questions were grouped according to outcomes from

Phase One. These three broad groupings distinctly broke down into various sub-themes during the coding process and are presented in Section 6.4.

The questionnaire, described in Chapter 5 (see Table 15) with underlying question groups is presented in Table 23.

Table 23

Phase Two Questionnaire

Q. No.		Question
1	Occupational Success	Could you explain how you started work in the security industry?
2		Could you explain your work experience?
3		Can you talk about the duties you undertake in your role?
4		Could you elaborate on the value security brings to your organisation?
5	Organisation Complexity	How complicated is your work?
6		Could you explain the unique stresses that come with a security role?
7		When you make decisions and start a task or project, is there a lot of uncertainty that you have to deal with?
8		Is the security environment changing faster now than it has been in the past?
9	Progression Ceiling	Could you explain what career pathways are open to you with your security experience?
10		How would you 'move up' in the organisation with a security background?
11		Do you think there is a point where security managers need to leave security to progress into more senior roles in an organisation?

6.3 Analysis

The analysis section provides direct responses to each question from the participant sample, identifying and articulating themes that were uncovered in the coding process. Subsequently, from this initial review of responses to the questions, the major and minor themes are extracted and presented in Section 6.4 in summary. The interview transcripts, with embedded coding are presented in Appendix E, and the combined coding table with key quotes, codes, and subsequent themes are presented in Appendix F. For brevity, these are not presented in this Chapter, with only key interview responses, discussion, and summarised themes presented.

6.3.1 Question One: Starting Work in the Security Industry

To the question: *Could you explain how you started work in the security industry?* participants responded in the operational Focus Groups that they came from various backgrounds. One such response was for participants to have started in the security industry as a security guard, and then working their way through the work hierarchy to their current positions. For example, O2LS states: "I was basically a security guard, started off doing door work…I was only 18 so, that was my first job." To counteract this view, a number of participants in these groups started their careers in aligned disciplines such as Law Enforcement or the Military. For example, O2SM stated "I did sixteen years in the British Army…it seemed the obvious transition from Army to civilian life." Other participants noted they began their security career after transitioning from other, non-related areas of work.

In response to the question, the executive cohort interviewed in the Focus Groups and Semi-Structured Interview articulated that they came from both 'traditional' police and military backgrounds, as well as non-typical corporate backgrounds. Most common were police, security, or military backgrounds; however, two participants came from law enforcement backgrounds, O1NH: "I was a police officer in Queensland Police and Federal Police for twenty-three years" and O2PM: I started in Banking…went into law enforcement for ten years, serious fraud office for two years," and two participants came from security backgrounds, O4DM: "How did I start? I started on a door, doing some door work like a lot of young islanders", and O4CC "I got into it originally as a surveillance operator at a casino in Melbourne." Others came from less typical backgrounds, such as O1AW: "I don't have a security background but was moved into a risk and security role as part of an organisational restructure." Overall, security careers seem to start in a variety of places, with non-security backgrounds, police and military, and security backgrounds each finding their way to the peak of the occupational stratum.

6.3.2 Question Two: Participant Work Experience

To the question: *Could you explain your work experience?* participants responded in the operational Focus Groups that they generally progressed to their current position from similar operational roles or from aligned disciplines. Almost all participants did not have a pure security background, with their starting careers being varied. For example, O1C states: "I started off as an accounts admin manager at a child care centre" and O4BB: adds "After finishing high school I went to a university and studied accounting…I joined the organisation as a table games dealer." Nevertheless, others responded with policing or military backgrounds, as identified in the response to Question One.

From the executive cohort, including the semi-structured interview, participants responded with both their educational and work backgrounds. Several executive participants were university educated and

had a history of security specific work experience as indicated in the responses to Question One. Nevertheless, some participants had broader risk or organisational experience, like O2PG who explains “My background is in risk management, crisis management, incident management, business continuity” and O1AW: “I ran a shopping centre in Victoria and about five years of experience…as a centre manager.” These diverse experience backgrounds are more typical of what would be expected of individuals operating in an executive position (Mumford et al., 2007).

6.3.3 Question Three: Security Duties and Roles

In response to Question Three: *Can you talk about the duties you undertake in your role?* The operational focus group participants responded with various supervisory and bounded tasks. For example, O1C states: “I run about 40 guards in the centre. Basically, looking after the guards”. Such a supervisory role is also completed by O1BG, who responds “I oversee C and his team in regards to all security related issues.” Furthermore, O4BB also supported this supervisory work, by stating: “We’re in charge of obviously monitoring our staff, making sure they hit their KPIs.” Such supervisory roles are typical of Stratum Two positions within the work hierarchy, and are very technical roles (Clement & Clement, 2013). Such work roles also align with those articulated by the security literature (Fay, 2002).

Nevertheless, not all tasks were supervisory in nature, with some participants responses highlighting operational procedures they had to comply with, for example O4SM: “One of the main roles would be managing patrons…we would have to manage self-exclusions [from the Entertainment Precinct],” as well the highly technical roles they fulfil, with O2MR explaining: “I look after all the design of [electronic security] in the organisation…what equipment is being installed…to keep people safe.” Such tasks are consistent with a Stratum One or Two seating as these activities are highly prescribed, process driven, and require input from higher order strata roles to conduct their work appropriately.

The executive cohort responded with higher order tasking’s and more generalist managerial responsibilities bounded within a technical discipline. For example, O1AW explains that their role has “moved from a very localised crime focus to an organisational security focus.” This higher order approach is reinforced by O1LT, who explains that part of their role is the development of organisational policies to support the security and intelligence function “There aren’t really any policies or standards that you can access anywhere so that you’re kind of developing those as you go along.” This systems development tasking is consistent with higher stratum seating within the management literature (Mahajan, 2010). Nevertheless, there was evidence of technical specialisation within these higher order roles, as articulated by O4CC: “I would say nearly 50-60% [of my role is] people management…the more technical side is then managing the actual operations of the CCTV

network." This technical focus indicates that executive security roles may not be as senior as their title suggests (Mumford et al., 2007).

6.3.4 Question Four: Security and Organisational Value

In response to Question Four, which was: *Could you elaborate on the value security brings to your organisation?* The participants responded with two overarching views, the first being that security fulfils a number of business focussed tasks outside of their core role on the ground, for example providing customer service. This view was articulated by O1BG, who states: "There's the big…preconception that security is just there to be a presence …where security actually does a hell of a lot more…it's very customer service focussed." In response, O1C agreed and elaborated, explaining: "99% of issues we get involved, if there's a fire alarm, we're the first responders, if there is a structural collapse, a floor, anything that has affected the centre, we as security will look after it as the first responder."

The second overarching viewpoint was the provision of comfort to staff and enabling other business functions. For example, O2LS responded by stating "I think we add that level of comfort for that event to run safely and without incident", and O4BB agreed, with "We also provide comfort, so people feel safe." Furthermore, this comfort allows the business to operate in a reduced risk environment as articulated by O2SH: "I think security enables a lot of other functions to exist." Both of these perspectives are captured in the literature and align with the articulated function of Corporate Security roles (Bamfield, 2014; Nalla & Wakefield, 2014).

From the executive cohort, respondents had a mixture of views, both supporting the concept of allowing business operations to function, but also to support customer experience and provide a level of brand protection. For example, O1AW explains "I think that our role and value that our roles play in security and our organisation is to allow our business to function regardless of the broad macro environment." Which is reinforced by O2PM: "I explain my role as reducing the impact on our people, our assets, and our business, and enabling our people to continue business in a safe manner." They continue "the CEO…said this team [security] deals with key moments of truth for customers. So our job is to ensure that customers retain confidence or regain confidence in the organisation." These views are consistent with the literature and promote the concept that security executives are planning for and controlling organisational risk exposure (MacCallum, 2013). Nevertheless, O2PG suggests that the value of security is not perceived by others in the organisation: "I believe security brings a lot of value into the organisation but it's largely unseen, and unrecognised." The value perception concern is also supported by the literature, with many lamenting the lack of impact security has on organisation strategy (Gill et al., 2008; McGee, 2006).

IDENTIFIED THEMES – OCCUPATIONAL SUCCESS

Overall, question one and question two revealed how participants entered the security industry, and their motivations for doing so. The identified themes from these questions included: interests and motivations to enter the industry, the classic pathway and the non-typical pathway into industry. These themes carried across both operational and executive strata interviews and focus groups.

Question three revealed the type of work tasks participants undertook, and thus their overall alignment within the occupational stratum. The identified themes from this question included three significant groupings of tasks, including: operational security roles, professional security roles, and tactical security roles. These themes were identified through analysis of both operational and executive strata interviews and focus groups.

Finally, question four revealed participant views on the value adds to the organisation, both their perception of the value added, but also the perception of others within the organisation of that value. Subsequently, the question spawned several themes, including the concept of security being integral to business operations, as well as the idea that security provides comfort to staff and clients. Further, themes included the lack of recognition of security, as well as the difficulty in measuring security outcomes.

6.3.5 Question Five: Complexity in Security Work

In response to the Question: *How complicated is your work?* Operational focus group participants responded in general agreeance to that dealing with internal and external stakeholders adds to the complexity of their roles. For example, O2SH explains that "The size of the organisation, and finding the right people…you can't get anything done without knowing the organisation [which adds to the complexity]," such a view is reinforced by O1C who elaborates: "There's about forty managers that you have to report to so that's one of the complicated bits you know." The participants concern about meeting the organisational system requirements; coordinating, seeking permission from, and then acting strongly aligns with lower strata work (Mintzberg, 2009). The interviewees indicated that they were bounded within their defined set of responsibilities, and managing the inputs received by superiors to enact their role added to the felt complexity in the role. Nevertheless, the executive cohort also commented on the complexity of dealing with people, but in the context of leadership and influence as opposed to direction and coordination.

Subsequently, the executive cohort generally agreed that the complexity or difficulty in their roles came primarily from influencing and leading people within the organisation to support their

objectives. O1AW explains that the "complications come from being able to influence other internal stakeholders who may not see security as a big a priority." To support this view, O2PM adds that "when you're dealing with people it's inherently complex. So, when we're looking to provide systems, and processes, and equipment to support people to remain safe and secure, that people factor just introduces the complexity." This viewpoint was reflected by the majority of executive participants across all the focus groups and the semi-structured interview. The shift in focus from coordinating delegated responsibilities from several stakeholders to attempting to influence stakeholders to enact security objectives is a noticeable and important indicator of higher order strata seating (Deming, 2013).

6.3.6 Question Six: The Unique Stress of Security Roles

In response to the Question: *Could you explain the unique stresses that come with a security role?* The operational focus group participants varied in their responses ranging from operational issues, shift work to stakeholder involvement. For example, O1BG explains the pressure of hierarchy oversight "One of the biggest stresses here…is having national support and head office and the directors in the building. So, when an issue does arise, they're getting involved straight away." O2SH explains a similar pressure, but from the perspective of blame: "if something goes wrong the security has failed, so when that happens more often than not people want to look, they want to blame." These concerns were not mirrored by participants in Organisation Four, who explains that their stress lies in the requirement for shift work, with O4SM elaborating: "12-hour shift work can be quite stressful, particularly those working nights. It's full on." These differences could be attributed to the organisation structure and operating context; Organisation Four being an entertainment precinct and Organisation Two being a banking institution with different requirements, stakeholders, and operational overlays.

The executive cohort responded with a few supported views, those being the stress of being responsible for the security of the organisation 24/7 and also the stress of having inadequate resources or poorly trained staff to carry out the function's requirements. O1LT explains the stress of 24/7 availability, "with roles here…it's 24/7 that we need to be on our phones, engaged, available, at all times. I think that does definitely take its toll after a while" which is reinforced by O2PM and O4CC. The constant availability is a common theme throughout the occupation strata, and is consistent with security literature (Sennewald, 2011). From a resourcing perspective, both O2SM and O2PG agree that one of their role stresses is the lack of appropriate funding or appropriate staff to achieve their objectives, with O2SM stating "One of the stresses we have are the people at the moment who we've inherited…we're stuck with the people who've exceeded their levels of incompetence," and O2PG reinforcing this view from a monetary resource perspective "We've been seen as an overhead. Right,

so we've been cut cut cut cut cut, so it's—security is not seen as a business." These concerns echo the perceived value perception from others within the organisation; value perceptions can substantially impact resourcing, and success in lobbying for security objectives (Gill et al., 2008).

6.3.7 Question Seven: Uncertainty in Security Decision Making

Question Seven was: *When you make decisions and start a task or project, is there a lot of uncertainty that you have to deal with?* The response from the operational focus group cohort resulted in numerous participants agreeing that there is limited uncertainty in their roles. For example, O1BG explains that "I wouldn't say there's uncertainty…there has to be a lot more consultation just in regards to the asset as a whole." This is reinforced by O2MR, who elaborates "We have the freedom to make decisions if it's in our space…we have installation standards and guidelines, but we base some of it off a risk assessment." These responses suggest that while the participants have some decision-making authority, they are wholly bounded by consultation and guidelines for implementation. Importantly, O1C supports this view by explaining that they are bounded by a generic predefined response and raise an exception if needed: "The guards are trained to make a generic response, or they just wait for more of the experts to come on site to kind of take-over." All of these elements strongly align with lower strata work, and reflect the expected process driven nature for such roles (Jaques, 1996).

The executive cohort, however, identified uncertainty around decision making, particularly when it is viewed after the fact, aligning with the expected influence and leadership elements of such roles (Mintzberg, 2009). For example, O2PM explains that the basis of their role is working in a sub-optimal information environment. This sub-optimal information environment requires the individual to exercise their judgement, but the response to that judgement by other decision makers after the fact is uncertain. As O4CC explains "The uncertainty would probably be in how it's [the decision] viewed later on…but I wouldn't say there is uncertainty around what my decision would be." Such a view is reinforced by O4DM "You find yourself making decisions with very little information…when things just happen you don't have the information, and that information is obviously there on Monday morning." The progression in uncertainty from operational to executive roles is expected, and demonstrates a shift in understanding, appreciating, and forecasting of consequences.

6.3.8 Question Eight: The Rate of Change

In response to the Question: *Is the security environment changing faster now than it has been in the past?* The operational focus groups generally agreed that the increased awareness of terrorism has led to a faster changing security environment. O1BG explains "there is a higher risk of terrorism obviously around the world which is impacting a lot of security operations," and this view is reinforced

by O2LS who explains in their previous role that "As soon as Australia went into high alert, there were all these things that were implemented over there [at the previous employer], and it evolved really really quickly, like bollards, and then 100% bag checks." Further in agreeance is O4SM who states: "I think [the threat environment changing is] inevitable though, especially with the current climate in relation to the threat of terrorism." Such a change in operating environment could have an impact in the ability for participants to forecast and thus reduce their time span of discretion due to increases in operational requirements and increased stress (Clement, 2015).

Subsequently, the executive cohort in the interviews and focus groups agreed that the security environment had shifted, with most agreeing that it had quickened and become more complex with new threats. O1AW explains their perspective "[the threat environment] it's evolving on a daily basis and you know….incorporating cyber as a rapidly increasing risk to our operations and the global environment...[with] low sophistication terrorist incidents…absolutely the environments evolving faster now than ever," which was supported by the rest of the cohort. Further, there was general agreeance that the non-security executive does not fully appreciate the current environment, with O4CC articulating: "I don't think the level above us probably understand it, and I don't think they probably will until the worst case scenario hits" which is reinforced by O2PG "Their [the executive] awareness level is low." This view was relatively common amongst the cohort, and again aligns with the concept of an undervalued security function.

IDENTIFIED THEMES – ORGANISATIONAL COMPLEXITY

Overall, questions five, six, seven, and eight revealed several aspects of the participants roles that contributed to their feelings of complexity. Such aspects of complexity were grouped into themes, which included the operating environment of the organisation, work hierarchy influence in their roles and tasking, and the inherent role complexity stemming from duties and processes and the ways in which these are implemented. Complexity found within the organisations operating environment included the 24/7 nature of security roles, the shift in security posture to meet new threats, the pace of technological change, and the difficulties of dealing with the unknown. The complexity identified in the work hierarchy included the rapid change in priorities and expectations of security from others in the organisation, as well as the felt interference of these other stakeholders in security activities. Finally, the complexity articulated in security roles ranged from dealing with people and exerting influence, through the breadth of responsibility, delegating decision making, and applying technical skills within a highly bounded occupation structure.

6.3.9 Question Nine: Career Pathways in Security

To the question: *Could you explain what career pathways are open to you with your security experience?* The operational focus groups had mixed responses to the question, some identifying plenty of opportunity for future career progression, and others feeling less confident. The participants in Organisation One were confident about their career prospects, with O1C explaining: "There are a lot of pathways, just [pick] one of them that interests you in the end—if you're always willing to improve yourself [you'll progress]," and with reinforcement from O1BG: "I think the security role is actually one of the most diverse roles to move forward, because you have a good touch on each of those areas within the business. You can add value to any other business." Organisation Two participants largely agreed, with O2LS explaining that their progression to date demonstrates the opportunities available, and O2SH summarising "I suppose that's what's good with the world going to shit—we get more job opportunities." Nevertheless, O2MR explained some of the difficulties in starting or progressing in security careers "it's very difficult though, to be able to get into the industry and depending on where you want to go, there's no set course into any of the security jobs," and this view was supported by the participants from Organisation Four who felt progression within their organisation would be more difficult. Overall this mixture of viewpoints could largely be dependent on the perceived value of security within the organisation, or the inherent room for promotion within the technical occupation strata (Speer, 2017).

On the other hand, the executive cohort had quite different perspectives on career opportunities. In terms of their own career progression, the cohort was mixed with some identifying relatively good opportunities to step into broader roles outside of the security occupation, and others articulating a progression ceiling. For example, O1AW explains the wealth of experience that would facilitate a role change: "the skill set that the [security executive] team or most roles within our team have is applicable and can add a lot of value to other areas of our business," such a view is reinforced by O4DM. Nevertheless, O2PG suggests they have reached their peak "I'm probably capped at where I would be…but given the current, and I'll call it a glass ceiling, in terms of getting up into the executive, I don't know of any corporate that actively has an executive or a board member who has a pure security background." This ceiling is further identified by O4CC and O1NH, and O2PM who explains: "I don't see a linear promotional line, it is rare to see security people end up being CEO's of non-security type companies." This mixed response likely speaks to the organisations structure and incentive schemes, as well as the level of technical speciality the participants have. Those with broader backgrounds articulated more optimism to those with deep technical expertise in the occupation.

6.3.10 Question Ten: Progression in Security Careers

In response to the Question: *How would you 'move up' in the organisation with a security background?* The operational focus group participants had a variety of views, with some suggesting that staying in their current position would be more beneficial, and others suggesting that leaving security would be better. For example, O1C did not see the value in stepping sideways "if I were to move sideways it would be the same role somewhere else." and this was supported by O1BG: "I think staying in my current role would help me progress more." Nevertheless, O4SM in Organisation Four saw more opportunity in moving to other areas within the organisation: "To be honest there isn't really any further advancement…if I wanted to progress it would be in another part of the [organisation]," and this view was supported by O2SH: "yeah there's a lot of these opportunities…to move within the company [into a different occupation] but not have to worry about starting all over again." Again, such views likely align with the incentive structure within the organisation for security careers; those with limited progression opportunities are likely to reward sideways movement earlier than those with stronger and more developed progression offerings (Strauss, 1975/2001).

Executive participants had differing views from the operations cohort, as O2PM points out, education can be an important factor influencing progression. They state that "Some of my direct reports, I've encouraged them and promoted them through to MBA's so that they gain a general business understanding…it also gives them more generalist skill sets." O2PG agrees with this view, adding that broader generalist and people skills are vital for progression beyond lower strata roles. Generally, this view is supported by the executive cohort as a whole, as well as the literature. Education is a substantial influencing factor on career progression, and it is not unexpected to see such a view being reinforced by those in executive roles (McGregor, 1997).

6.3.11 Question Eleven: Ceilings in the Security Occupation

In response to the Question: Do you think there is a point where security managers need to leave security to progress into more senior roles in an organisation? The operational focus groups had a view that while security can exist in higher reaches of the organisation, it gets more limited. For example, O1BG: "Security does go all the way to the top, it just gets a little more limited the higher you go, in regards to opportunities…a lot of companies or people in management looking at those senior roles, they immediately go to someone with defence or policing experience." Such a perception of a limited career opportunities in security is reflected in the executive cohort and reinforced in the organisational literature—specialist roles typically do not have strong progression pathways within organisations (Strauss, 1975/2001).

From the executive perspective, broadening into non-security areas is vital, even though a specific level of seniority could not be identified for such a move. O4CC explains "I think its maybe you probably need to move to a different business unit or do a secondment whether it's through a project team or putting your hand in something that goes out of your technical knowledge." Such a view was supported by the executive cohort as a whole, with many seeing this as an opportunity rather than a career blocking arrangement. For progression within the security occupation hierarchy, O2PM summarises it "yes [the security occupation] it is narrow, there is only one spot at the top, and I have to fall off my perch before someone can step up."

IDENTIFIED THEMES – PROGRESSION CEILING

Overall, questions nine, ten, and eleven, revealed several underlying themes around the ability for security specialists to move up within the occupational hierarchy, and within the broader organisational strata as a whole. The themes identified included participant perspectives around the limitations of a security career, including a felt progression ceiling, and the poor standards of individuals within the occupation, as well as a theme around opportunities for those with security careers. Such opportunities included lots of pathways for advancement, in opposition to the limited career options espoused by some participants, the benefit of broadening human capital skills in advancement opportunities, and the diversity of skills developed in security careers.

6.4 Themes

The section outlines the identified themes that emerged from the question responses. The section further provides analysis of the responses within these theme categories, drawing initial links to the literature for further discussion in the interpretation presented in Chapter Seven.

Subsequently, the major identified themes presented below include Occupational Success, Organisational Complexity, and Progression Ceiling, aligning with the question categories presented in Section 2.1.

6.4.1 Theme One: Occupational Success

In review, the study sought to understand the extent to which security careers saw occupational success, and if so, how those careers commenced. Such an understanding is important in responding to the research questions, particularly to understand the extent to which there is a progression ceiling in the occupation. Importantly, the literature, for example Oesch (2015); Speer (2017); and Weeden (2002), suggests that occupational success can be closely tied with social class and alignment of the occupation to core business activities and profit making. Subsequently, the sub-themes that emerged

from the interviews were those relating to career pathways, and the interests and motivations behind starting such careers. It is acknowledged that substantial education data was collected from the participants, and such a background further adds to the understanding of class and social standing of the participants. Sub themes identified under Theme One included the following:

- The start of a career;
- The 'classic' pathway into the security occupation;
- The 'non-typical' pathway into the security occupation;
- The role of education in the security occupation;
- Operational security roles: Implementation, compliance, and supervision;
- Professional security roles: Horizon scanning and management;
- Tactical security roles: Direction, influence, and security policy;
- Tactical security and managing business units;
- Value perceptions of the security occupation;
- Security in support of business operations;
- Security as a comfort provider;
- The lack of recognition of security; and
- Measuring security.

It was clear from the analysis that the majority of security careers begin in aligned, or perceived aligned disciplines such as police or military occupations. While there was evidence of those coming from other backgrounds, such as management or sales, these instances were the exception. Nevertheless, the cohort was relatively well educated, particularly at the peak of the investigated organisations, suggesting that a domain specialist background paired with the appropriate levels of education lead to a higher likelihood of success in career advancement. Such a finding aligns closely with McGregor (1997) whom suggested education was a key factor in class and societal progression, particularly in Australia.

Further, the analysis uncovered three broad categories of security roles, which included those operational security roles that involve 'concrete shaping' tasks that are highly process driven (Clement, 2015), as well as professional roles and tactical roles. Professional roles included work tasks that required longer term thinking and more analytical thought; there was room to formulate new approaches and methodologies within a bounded operating environment (Ivanov, 2015b). Finally, tactical roles were more aligned with general managerial tasks, including a strong focus on shaping the direction of the security function within the business, with a focus on protecting the organisation as whole (Craddock, 2002). Though these roles were deemed tactical in nature, they did not include traditional strategic managerial roles such as detailed market analysis, product generation, or broader business planning (Papadakis et al., 1998); uncovered taskings seemed to be specific to security and the protection of assets only.

Subsequently, the analysis uncovered the importance of the perception of security value to the broader business, but also to the security function as well. The concept of the security function providing 'comfort' to the business and its staff and customers was articulated by many participants and speaks to the idea that security enables the business to function without undue fear or concern about disruption from human threats. Nevertheless, those in executive strata seatings found in some instances that the security function was undervalued by business decision makers, leading to difficulty in providing the appropriate level of protection to the organisation. Overall, this could be attributed to the difficulty in measuring security provision and its effectiveness in reducing risk.

6.4.2 Theme Two: Organisational Complexity

The study sought to understand the complexity and uncertainty found within Corporate Security function as stress, complexity, and uncertainty substantially relate to the levels of work found within organisations (Craddock, 2002). Stress or reactionary approaches to work can lead to reduced time span of discretions (Clement, 2015), and thus a compressed decision-making hierarchy. This aspect was investigated to determine the types of stressors that security practitioners could experience and the impact on their work.

The three main sub-themes identified that outline the complexity found within the Corporate Security occupation strata relate to the operating environment that the organisation is in, the organisations hierarchy, and the expected role of the security practitioner.

Nevertheless, these sub themes further included the following:

- Complexity found in the operating environment;
- Complexity found in security operations;
- Managing and changing the security posture of an organisation;
- Dealing with the unknown and uncertainty;
- Work hierarchy structure and its influence on the complexity of security roles;
- Dealing with people;
- Delegating decisions;
- Applying unique security skills within an organisation; and
- Breadth and depth of security roles.

Overall, security roles were determined to be quite complex for a variety of reasons, including the demands of the operating environment, uncertainty when dealing with people, and the continuously changing threat environment. This complexity suggests that while security practitioners may be operating within a relatively short time span of discretion as uncovered in Phase One, their felt complexity results in higher-order decision making that may more closely align with higher strata positions (Clement & Clement, 2013). Whether this felt complexity is recognised by organisations or

not is unknown, which may result in lower structural seating than expected for the roles difficulty. Nevertheless, security roles were found to be complex due to the substantial uncertainty found in working with people and trying to reduce the risk of people-based problems from occurring. For example, some participants noted that the security threat environment has changed dramatically over the last few years and continues to do so, requiring their teams to be highly agile and capable of responding quickly. In large organisations this means practitioners need to manage substantial internal relationships, and balance business needs with security outcomes (Gill et al., 2008).

Overall, security roles were uncovered to be quite broad in their remit, and practitioners were required to have a deep knowledge of several disparate functions (Interim Security Professional's Taskforce, 2008). For example, facility management, emergency management, security, and customer service being but a few. Consequently, further complexity arose when delegating these complex and multi-role functions to other staff, who some participants noted were (in lower strata seatings) undertrained, undereducated, and inexperienced. This leads to those in higher order managerial positions to get 'pulled into the weeds' and take part in operational decision making and operational activities where this should be managed by junior staff.

6.4.3 Theme Three: Progression Ceiling

The final series of questions sought to uncover information about career progression pathways within the security occupation and any progression ceilings within the discipline. The main themes uncovered from the interviews included what is termed the limited career, which elaborates on perceptions of progression ceilings and poor standards within the occupation. Next, several opportunities were identified that could allow for career progression beyond these identified ceilings under the right circumstances; particularly if individuals were to leave the security occupation.

Subsequently, the sub themes included:

- The limited career and progression ceilings;
- Poor standards in the industry and its impact on progression opportunities;
- Pathways for progression.

In review, the analysis uncovered that the security occupational stream can be limited for opportunity, particularly at the more senior ranks. Some of this restriction stems from the deep specialisation found at the higher end of the work stratum, but also due to the limited number of job opportunities. Furthering this, several participants identified a lack of consistency in quality, education, and experience of candidates, including the poor standards of training. These elements of the security workforce could have substantial impacts on career progression opportunities.

Nevertheless, some participants did identify opportunity for career progression, articulating the variety of skills needed in a security career, and how this could help individuals progress into other areas of the business. Subsequently, it is theorised that individuals starting in the security industry are exposed to a wide range of skills and are required to develop the capacity to deal with substantial uncertainty. If these individuals were to leave the security work strata and move into other areas of the business, they may have more opportunity to progress into higher order positions within the organisation than if they remained in the security function (Speer, 2017).

6.5 Reliability and Validity

The Phase findings are braced by a robust approach to reliability and validity. As articulated by Stewart et al. (2007, pp. 118-125) consistency in data collection and analysis are paramount in focus group methodological approaches due to the variety of responses possible from participants. To address this consistency considerations, the focus group participants were asked the same questions priori developed from the preceding phase, with subsequent prompting in accordance with semi-structured interview techniques (Qu & Dumay, 2011). Further, a consistent analytical process was undertaken during coding, as depicted in Appendix E and F (Saldana, 2009), and this is additionally supported by the provided transcripts of the interviews and focus groups as the researcher's interpretation of the data can be reflected upon in light of the raw data (Bloor et al., 2001, pp. 42-43).

Nevertheless, articulated by Sutton and Austin (2015), qualitative research requires substantial reflection before, during, and after data collection to provide context to the analysis of findings. As bias in qualitative research is unavoidable due to the nature of human-to-human interactions such as that found in interviews (Qu & Dumay, 2011), a clear articulation of potential bias sources allows the reader to make their own judgements about the reliability and validity of the researcher's assessment. Such a statement of researcher biases and subjective lived experience should consider various sociological, epistemological, and methodological assumptions. Therefore, Section 6.5.1 provides a bias statement for consideration. Furthermore, the coded transcripts and coding table found are provided in Appendix E and Appendix F for the reader to interrogate as required for validity and reliability purposes.

6.5.1 Researcher Bias Statement

Upon reflection several sociological biases were identified. The researcher is currently employed in the security occupation as an independent security consultant working for a large multi-national firm. Furthermore, the researcher has previously held positions within a Corporate Security function for a large international firm and has over five years of experience in security electronics, security

management, and security consulting. Such experience in the workforce can shift perceptions of the relative importance of security roles.

6.6 Conclusion

The Chapter presented the outcomes from the second phase of the research. Phase Two included several focus groups and an interview with individuals from three Australian organisations. The participants included those from the organisation's executive teams, middle managerial teams, and the operational teams within the security function. The Chapter then presented the themes uncovered through these interviews and focus groups.

The identified themes included the relative success of the security occupation within organisations within the bounds of a functioning business unit. This included operational, professional, and tactical taskings across the work strata. Importantly, these roles appear bounded by the organisations structure which is influenced by the ability for the function to demonstrate and measure its worth in the organisations business. Subsequently, the success of the security occupation is bound with its ability to communicate within the business environment, however more broadly organisations tend to value individuals with deep domain speciality from military and policing backgrounds over more generalist individuals, thus limiting their ability to communicate in relation to broader business objectives.

Further, the impact of organisational and role complexity was explored, with several themes uncovered. This included the complexity found within such bounded organisation structures; due to the uncovered specialisation of security managers and executives, there is a tendency for these individuals to get pulled into operational matters, restricting their ability to plan longer term and engage in business shaping activities. Furthermore, as security is focussed on managing people and people's behaviour, there can be substantial uncertainty in the role, contributing to decision making anxiety. These factors all influence the individual's capacity to forecast into the future (and thus increasing their time span of discretion and improving their position within the work hierarchy).

Finally, Phase two sought to understand the potential occupational progression ceiling for security practitioners, with several supporting themes found. In consideration of the above-mentioned factors, those being the organisations perception of security value, the inherent specialisation of executive and senior managers, and the limited integration with business objectives and processes, the security occupation could be limited in progression, particularly for those who have no experience outside of the domain. As the managerial literature suggests, domain specialists are less likely to be promoted into the higher reaches of an organisation than generalists, and the phase findings suggest that even at the highest reaches of the security occupation, generalist skills were less developed than

expected. The roles uncovered at the ‘executive’ level of the function were more aligned with general managerial roles in charge of discrete business functions as opposed to strategic business managers charting a course for the organisation writ large.

CHAPTER SEVEN

INTERPRETATION AND DISCUSSION

7.0 Introduction

The Chapter presents the interpretation of the phase data analysis in response to the Research Questions. This interpretation includes the identified stratum of work for Corporate Security within Australian organisations, the ability for the Corporate Security function to influence others within the organisation (i.e. permeate across functions) and articulates the uncovering of a potential progression ceiling for the occupation. Accordingly, the study found three distinct role orientations within the Corporate Security stratum of work; the operational, professional, and tactical role orientations, with these being aligned across a stratum of work stretching from Stratum One through Four. These roles and hierarchical positions can influence various decision makers across all levels of the organisation, but find complexity in the variety of tasks to be completed, competing expectations from decision makers, and struggle to receive organisational buy in. Finally, an occupational ceiling was uncovered for Corporate Security practitioners.

Overall, these findings are reinforced by various literature sources, including the socio-organisational, career, and security literature (Brooks, 2013; Jaques, 1996; Strauss, 1975/2001). For example, the uncovered Corporate Security stratum of work is supported by the socio-organisational literature, where technostructure roles fulfil work managing business units and operate in reducing uncertainty for business operation (Mintzberg, 1979). The uncovered security roles within this stratum of work align with the expectations from the security literature, (Nalla & Morash, 2002), though there is disagreement about where these roles should be located along the work hierarchy. Subsequently, the uncovered security influence and cross-discipline engagement throughout the organisation was also supported by the organisational and security literature sources (Brooks & Coole, 2017; Mumford et al., 2007). Finally, the identified occupational ceiling for Corporate Security practitioners is strongly supported by the career and organisational literature (Maitland & Sammartino, 2014; Sammarra et al., 2012; Speer, 2017). In short, these findings and their interpretation are presented in The Chapter below.

7.1 The Corporate Security Stratum of Work

The study sought to investigate the underlying stratum of Corporate Security work within Australian organisations. In aid of this investigation, the study posed the Sub-Research Question: *What is the corporate stratum of security practitioners in the Australian organisational context?'*

In response to the first sub-research question, the study found that a stratum of work does exist for Corporate Security within the Australian context. This stratum, as outlined by Jaques (1996), includes a hierarchy of activities aligned to four role seatings. Where the security literature expects a strategic stratum position (Bayuk, 2010), none were found in this study. The uncovered strata seatings were aligned to a technostructure positioning within organisations due to their specialist function in reducing security uncertainty and security risk exposure for organisation activities (Galbraith, 1985). The discovered work strata arrangement is aligned to the work of Mintzberg (1980) and Jaques (1996) alongside others and presented below in Figure 15 (Jesus et al., 2015; Le Grand & Tahlin, 2013).

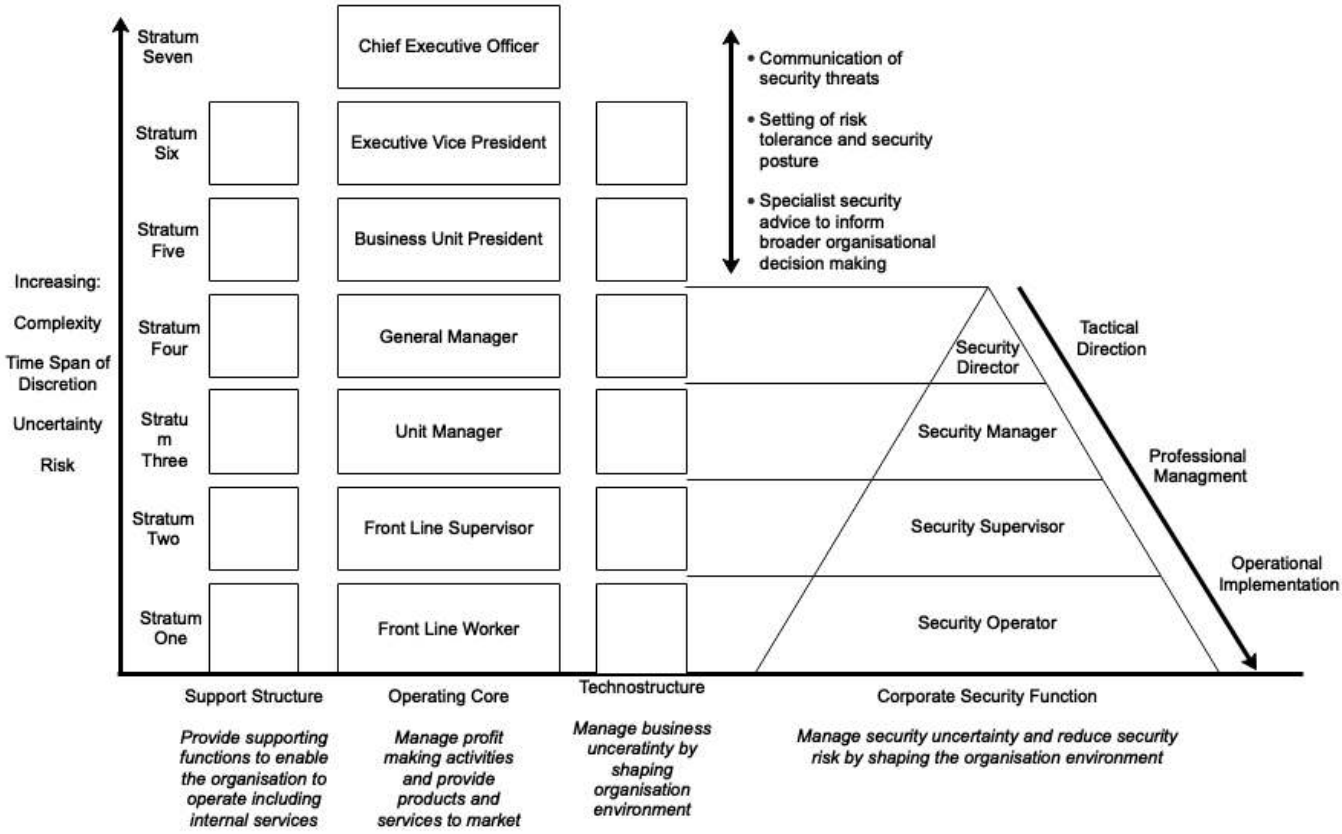

Figure 15. Study Findings

As found, the Corporate Security stratum of work operates from a tactical positioning with its peak at the General Managerial level, receiving overall direction from strategic executive decision makers. This structure is supported in the broader literature, for instance Papadakis and Barwise (2002) found that strategic decisions guide tactical planning through an assessment of the overall operating environment from a pure generalist perspective (Maitland & Sammartino, 2014). Then tactical planning and resourcing guides and supports the achievement of operational outcomes through the

translation of the broad strategic direction through professional functions (Jaques, 1996). In this model, strategically, the risk tolerance is set through liaison with specialists at the tactical level, and then at the tactical level policies and procedures are developed to mitigate risk concordant with tolerance levels (Somerson, 2009). Following, these policies and procedures are enacted and managed through professional roles whom engage directed mitigation strategies through operational task outputs (Bamfield, 2014).

7.1.1 Uncovered Security Roles

Several hierarchical Corporate Security roles were uncovered in Australian organisations, being Stratum One (Operational), Two (Supervisory), Three (Managerial), and Four (General Managerial). These roles articulate the Corporate Security stratum of work and align to the time span of discretion measurement articulated by Jaques (1996), as well as the descriptors of their expected role complexity (McKinley Advisors, 2018). The study did find some overlap of complexity around the Stratum Two and Stratum Three level of work; for example, some roles being oriented towards operational, professional, or tactical activities when sharing a Stratum Role category, which suggests some organisation compression or misalignment (Ivanov, 2015a). These complexity findings are discussed in more detail in response to the second Sub-Research Question. Nevertheless, the identified security roles are articulated below by their Strata descriptor.

7.1.2 Stratum One – Operational Security (Security Implementation)

Stratum One roles are found to generally be roles that are very action focussed and concrete in their descriptors (Clement & Clement, 2013). Across all participating organisations those who indicated Stratum One level work indicated that they undertook security activities that closely aligned with the identified, operational functional orientation. The majority of activities described at this stratum related to operational tasks such as rendering first aid, signing off reports, monitoring CCTV, and managing incidents. For example, as explained by one of the security officers interviewed, "*99% of issues we get involved, if there's a fire alarm, we're the first responders, if there is a structural collapse, a floor, anything that has affected the centre, we as security will look after it as the first responder.*" Such an articulation of Stratum One security roles is consistent with the overarching security literature (Brislin, 2014; Nalla & Wakefield, 2014).

Overall, individuals at these strata of work were implementing security strategy on the ground through concrete action and bounded decision making. These tasks are fulfilled for compliance with policy and procedures, with little opportunity to move beyond these internal organisational structures and respond dynamically to emerging issues (Grobler, 2005; Nalla & Morash, 2002). Such operational requirements also include supervision of others in the process of fulfilling these implementation

requirements. These findings mirror the security literature, with MacCallum (2013, pp. 6-7) describing these work areas as “basic personnel – technicians, operators, and security guards”, as well as “team leaders and security specialists.”

Subsequently, it was found that individuals operating at this stratum of work were not forecasting far into the future (days to months), and had a limited appreciation for higher order risk management decision making or mitigation strategies. Nevertheless, the security roles noted in the lower strata of work do however, seem to be quite diverse in their expected roles and thus seem to permeate within the technostructure roles outside of security, for example within facility management type taskings (Brooks, 2011). Furthermore, some security officers indicated that their roles included customer facings, service style roles. Such a diversity of taskings at this level of work suggests that as an ‘on the ground’ contributor, security is crossing between natural boundaries of work.

7.1.3 Stratum Two – Supervisory Security (Security Control)

Stratum Two roles are considered in the socio-organisational literature to be front line managerial roles, such as workforce supervisors (Craddock, 2002). Roles at this level of work operate within a time span of three months to one year, which allows for some short-term workforce planning, provision of some risk mitigation strategies, and other such tasks (Rowbottom & Billis, 1977; Sennewald, 2011). The findings from this study are consistent, in that those security roles identified as part of the Stratum Two work level were strongly aligned to this time span of discretion and expected activities.

Furthermore, Jaques (1996, p. 66) highlights Stratum Two roles as being ‘bigger picture’ with the requirement to “accumulate and consciously sort… data to diagnose emerging problems and initiate actions to prevent or overcome the problems identified”. These activities occur in different ways for both the operationally oriented Stratum Two’s and the professionally oriented individuals.

However, it is noted that Stratum Two roles across the different organisations were oriented in different ways. For example, some Stratum Two security workers were wholly bounded within operational work activities, working within defined procedures, and responding to incidents (Clement & Clement, 2013). Others however, were found to have a broader view, orienting their activities towards professional activities such as directing staff, interpreting policy into actionable risk mitigation strategies, and synthesising disparate information streams into workable knowledge (Brooks & Corkill, 2014). These differences in work activity within the same strata of work suggest uncertainty in the role’s responsibilities, and perhaps structural misalignment in the organisation (Ivanov, 2011).

7.1.4 Stratum Three – Specialist Managerial Security (Security Management)

Stratum Three roles are those that are responsible for the development of new systems and procedures, prescribing work to the lower strata of operations within the security function (Jacobs & Lewis, 1992). Such roles focus on solving internal problems with a specialist skill set; however, individuals at this level have begun to move to a more generalist management approach to problem solving (Jaques, 1996; Mumford et al., 2007). The results found roles such as 'Security Manager', 'Technical Manager', 'Security Operations Manager' as being listed by individuals assessed at this level (Bamfield, 2014; Burnstein, 1978).

Subsequently, Stratum Three roles articulated tasks that were longer term and more complex from those found in Stratum Two, typically aligning to activities in the professional and tactical functional areas of security work. Such activities included managing staff to achieve various objectives across a time span of years, as well as complex environmental scanning, building relationships both internal and external the firm, and overseeing contractual relationships. As Jaques (1996, p. 67) describes, activities and decision making that align to this level are those that "encompass the whole process within a plan that has a pathway to goal completion… [including] pre-planned alternative paths to change if need be."

Typically, the Stratum Three roles uncovered were focussed on guiding the implementation of security risk management strategies. Receiving direction from higher order roles (Stratum Four), interpreting a direction, and then delegating responsibilities down to the lower strata of work.

This approach to security work incorporates several strategies to manage and mitigate security risk, through the outsourcing of certain tasks through to the development of systems and procedures. In this instance, the security role involves a wide range of external environment scanning and the implementation of this complex information into the development of new systems. Noting the strong technical speciality found within these roles provides insight into the bounded nature of the security occupation within organisations (Ludbey & Brooks, 2017).

7.1.5 Stratum Four – General Managerial Security (Security Direction)

Stratum Four roles require strong managerial skills and the ability to operate as a generalist within a specialist domain; being unable to set strategic direction but being capable of influencing the way these strategic goals are determined and achieved at a tactical level (Maitland & Sammartino, 2014; Mumford et al., 2007). Decision-making generally occurs on tasks that could take between two and five years for their impacts to be seen. Security individuals at this level of work would be expected to be implementing longer-term security strategies to meet organisational objectives, for example interpreting and setting policy into actionable security strategies with respect to the organisations risk

tolerance, and feeding relevant threat and risk information to the executive strata for strategic decision making (MacCallum, 2013).

It is clear that security activities carried out in Stratum Four roles require authority and influence to direct and shape the organisations risk exposure to security threats (Cubbage & Brooks, 2013). For example, as one participant describes "*I get paid to exercise my judgement…I have career limiting conversations with important people in the organisation*." To achieve this clear direction, individuals have to strongly demonstrate an understanding of the security function within the organisation and its purpose as whole, as opposed to specific sub-specialities within the discipline (Brooks & Corkill, 2014). Importantly however, is the clear specialisation within the security domain still found at this stratum of work (McKinley Advisors, 2018). While the role is broader, more complex, and functionally at the peak of the uncovered security function, individuals were still highly specialised and non-generalist in their view of organisational activities; aligning them strongly to technostructure roles (Jo, 2018).

With this in mind, the tactical tasks articulated by the participants align closely with literature articulation of general managerial roles (i.e. Strata Four/Five), and not higher order executive seatings that would be expected from their occupational title (Mintzberg, 2009). Thematically most participant's discourse highlighted operational and tactical level tasks and roles, consistent with the Phase One (Ludbey et al., 2017). For instance, all participants were heavily specialised in their area of expertise, and while they indicated some broader organisational skills such as implementing policy, making judgement calls, and setting strategic direction, it was always bounded within their discipline speciality, not from a broader organisational perspective (i.e. profit-making activities).

Furthermore, where broader organisational management roles were demonstrated, and the individual managed several distinct business units, they were all security aligned areas of speciality. In other words, the peak security roles were not strategic in nature (Deming, 2013; Ivanov, 2015b). Where higher order strategic management staff tend to manage several disparate areas of specialty as part of their portfolio (Clement, 2015; Papadakis & Barwise, 2002), security practitioners with executive titles did not. In review of the literature, where discipline specific strategic outlook is found, typically these roles align with general management type roles at the Stratum Five level as a ceiling, and as found in this study for security, at Stratum Four (Clement & Clement, 2013; Maitland & Sammartino, 2014).

7.1.6 Uncovered Security Hierarchy

In summary, the following stratum of security works was uncovered in this study (Table 24). Security roles are articulated according to their identified time span of discretion, their typical role taskings,

and their functional orientation within security occupational activities within large Australian corporate organisations.

Table 24

Uncovered Security Work Hierarchy

Stratum	Role	Description	Time Span
One	Security Officer, Surveillance Operator	Provide first aid, respond to incidents, and monitor CCTV.	One day to one year
Two	Security Supervisor	Threat analysis, manage client relationships, and manage small teams.	
Three	Security Manager	Manage security risk and oversee security operations.	One year to five years
Four	Security Director / Chief Security Officer	Development and delivery of security strategy and policy, represent organisation.	
Five	NA	Not found in the security hierarchy.	Five years +
Six	NA		
Seven	NA		

Admittedly, there appeared to be some misalignment with some identified roles falling into the tactical (and in some instances, the operational) strata holding executive job titles. For example, Stratum One roles with the job title “Operations Manager” or “Director of Surveillance”, or a Stratum Four role with the title “Security Officer”. According to Ivanov (2011) such misalignment could indicate organisational compression, where multiple levels of work are operating within the same strata, leading to conflict, inefficiency and mistrust. Alternatively, such misalignment could suggest a misunderstanding of the roles being fulfilled by the security role, leading to an executive job title for a role that is fulfilling the equivalent of a supervisory or general managerial function. In both instances, such a role-strata misalignment can lead to organisational dysfunction; if such conflict is limited to the security business unit alone, the consequences are an under-utilised security workforce (Ivanov, 2006; McGee, 2006), with room for substantial growth—particularly with the expansion of strategic security activities where they are currently limited by organisational bureaucracy. Where this misalignment

carries across the business into other areas, organisational dysfunction and inefficiency is rife (Ivanov, 2011). Finally, such uncovered misalignment could suggest erroneous responses to the instrument, or a miscalibration of the instrument.

7.2 The Permeation of Security in Organisations

The study sought to understand the boundaries and orientation of the Corporate Security stratum of work. While the hierarchical extent of the work structure was uncovered, it was necessary to capture its lateral power and its overall influence within the organisation in aid of understanding the possibility of a progression ceiling (Heslin, 2005; Johns, 2006). Such an investigation was prefaced with the Sub-Research Question: *To what extent does the Corporate Security function permeate throughout organisations?*

In response, the study identified that Corporate Security operators has some lateral power throughout organisations, but this is implemented in a variety of ways depending on the individual's level of work (hierarchical seating) and their approach to handling complexity (Craddock, 2002). In particular the study found security works to be oriented towards operational complexity, professional complexity, and tactical complexity, each within the organisational structure known as the technostructure (Galbraith, 1985). These orientations were not always strata distinct with individuals at the same strata level functioning with different orientations.

In view of these functional orientations, the way in which security influences across strata levels varies depending on numerous factors. For example, organisational buy-in, security posture, and organisational interference can substantially affect the ability for Corporate Security decision makers to influence across the organisation (Jaques, 1996). Equally important, findings indicate that the responsive nature of security activities across all levels of work lead to a focus toward 'on the ground' activities and domain specialisation, even at higher order work strata (Clement, 2015).

7.2.1 Security Function Orientations

As articulated, the study uncovered several functional orientations of security activities which align to the complexity of security risk and business activities undertaken by security roles within corporate organisations. As articulated by Jaques (1996) and Le Grand and Tahlin (2013), work consists of both the complexity of the tasks and the capacity (or time span of discretion) of the individual to complete those tasks and forecast into the future while managing uncertainty (or risk). In security roles, this complexity presents itself differently along the work hierarchy, and is experienced differently by different security actors (Bazerman & Moore, 2009; White, 2014). While all security practitioners within the occupation are experiencing and reacting to risk, the orientation and methodology for reducing or managing these risks varies depending on their capacity to forecast and manage

uncertainty (Ludbey & Brooks, 2017). Thus, while two individuals may have the same hierarchical role within an organisation, they may interpret and react to risk in different ways, resulting in a different orientation in their management strategy.

Interestingly, the identified orientations align with findings presented by McKinley Advisors (2018) in their investigation into Corporate Security careers in the United States. While they present these areas as hierarchical seating positions within an organisation, the findings of this study suggest that this articulation is only part of the story. In other words, Corporate Security roles appear to be paired with a functional work orientation that is aligned but not determined by their hierarchical strata seating. Such work orientations directly influence their interaction with other areas of the business and their ability to understand broader organisational objectives and problem solve within the organisation's direction (Papadakis & Barwise, 2002; Papadakis et al., 1998).

7.2.2 Operational Orientation

Operational security orientations are limited in their complexity when considering the inherent uncertainty in the application of security in this area (Nalla & Wakefield, 2014). Individuals operating within an operational scope are very responsive and have limited forecasting abilities, however they fulfil an implementation, compliance, and supervision tasking (Clement, 2015). They react to on the ground issues, and complexity arises within the bounds of applying concrete tasks, procedures, legislative, and regulatory frameworks to shifting and unique incidents.

These complexity bounds led to a restricted capacity for operational roles to influence business operations. Nevertheless, the study found that security practitioners with an operational orientation were often fulfilling tasks outside of the security domain such as customer service and facilities management (Brislin, 2014). Furthermore, operational oriented roles regularly liaised with police and emergency services, allowing them to facilitate and influence the response arrangements during security incidents within the bounds of their policy and procedure direction. In effect, operational workers were managing direct security risk through direct shaping of the organisations operating environment.

7.2.3 Professional Orientation

Professional security orientations focus on the interpretation of strategy, directing people, and managing risk across several areas of the security function. Uncertainty in this application area relates to risk forecasting, trend analysis, managing staff, and working with internal and external stakeholders (Jaques, 1996; Sennewald, 2011). Overall, professional security activities require individuals to manage multiple, often disparate tasks, with multiple feeds of information needing to be synthesised into a coherent risk picture. From this risk picture, professional practitioners are required to interpret

broader risk management strategies as directed by the tactical practitioners and action these strategies through operational practitioners (Jaques, 1996).

The study found that professional security roles were able to influence and direct the implementation of the security function across the business and had opportunities to guide other parts of the organisation (Andersen, Garvey, & Roggi, 2014). While the overarching security strategy for risk management is set at the tactical level, the implementation details of this strategy are defined and actioned at the professional level. In other words, they apply security systems and processes to meet broader security objectives (Sennewald, 2011). With this in mind, professional security practitioners build relationships with other parts of the organisation to introduce security requirements in line with the security posture. Thus, professional security practitioners are liaisons within the organisation, shaping the operating environment for the organisation through their input into organisational processes and direction of security operations (MacCallum, 2013).

7.2.4 Tactical Orientation

These systems that are managed professionally and then applied operationally are created as an outcome of tactical security activities. In the tactical application of security, roles become more complex, specifically due to the inherent authority and influence across all security areas within the organisation (ASIS International., 2004; McKinley Advisors, 2018). Roles seated within the tactical stream of security work create systems and policies as part of their management of long-term security risk trends. While ultimate direction and risk tolerance is set by the strategic executive ranks of the organisation, tactical security roles form part of the decision-making process, and then seek to translate this risk tolerance into security terms for enactment within the security strata of work (Maitland & Sammartino, 2014). As part of this systems creation, tactical security activities include the development of internal security teams (workforce planning), influencing other areas of the business, developing organisational resilience, and taking complete ownership of the entire security function (Brooks & Corkill, 2014). Tactical security roles are responsible for setting the direction of the security function within the business (MacCallum, 2013).

Subsequently, tactical security activities also include liaising with organisation executives to inform them of security incidents, trends, and changes to the security environment so they can incorporate these security factors into their long-term strategic decision making and planning activities (Talbot & Jakeman, 2009). While those oriented towards tactical security activities were applying generalist managerial skills such as planning, managing people, and building relationships within the firm, these skills were still wholly bounded within the application of security, and these activities are still guided by higher order organisational strategy that is set by the executive. Those organisations with a lower

risk tolerance to security incidents provide more opportunity for security practitioners at the tactical, professional and operation orientations to have more influence and authority across the organisation as a whole.

7.2.5 Security as Technostructure

As articulated, the identified Corporate Security stratum of work, alongside the role orientations lead to the concept of Corporate Security being a reducer of uncertainty and manager of risk. Specifically, the reduction of security risk that is oriented towards business operations (Walby, Wilkinson, & Lippert, 2014). As with all technostructure functions, Corporate Security is found to be a technical work stream, which guides and directs the implementation of a specific area to support business operations (Mintzberg, 1980). In the case of Corporate Security, this technical work stream relates to the self-protection of the organisation within a framework of risk tolerance that is decided by the executive.

It is noted that while security practitioners along the uncovered stratum of work do indeed progress from highly technical and specialist skills such as applying first aid, responding to incidents, designing electronic security systems and the like to more generalist managerial skills such as controlling, leading, and influencing, they do not progress from solving security problems within the organisation (Maitland & Sammartino, 2014). Where those outside of technostructure and support roles progress into executive managerial positions, they solve broader organisational problems not bounded by their domain speciality (Barnard, 1938/1971; Sadler-Smith & Shefy, 2004). This aspect is not true of security practitioners, and thus they have limited influence at the executive level.

Such a finding reinforces the security literature in several instances, including that security is functionally significant within large corporate organisations, and that is plays an instrumental role in allowing business operations to function and be resilience in the face of security incidents (Coole et al., 2017; Cubbage & Brooks, 2013). Even so, the findings also support the socio-organisational literature to the incongruity of the security literature in the view of security not being strategically significant (Papadakis & Barwise, 2002). The findings support the concept of security being a partner in strategic decision making, but not an integral part of the final determination. The security function provides information and guidance, but the strategic direction is set by others, which is then interpreted into a security strategy and direction by the security function. Such a finding is consistent with the organisational literature (Jaques, 1996; Maitland & Sammartino, 2014).

7.3 The Corporate Security Occupation Ceiling

In review of the two research sub questions, the study uncovered a clearly articulated stratum of security work and identified the influence and overall complexity of this work hierarchy within Australian organisations. Subsequently, the study sought to identify a security occupation progression ceiling (or lack thereof) to understand the extent to which security careers can lead to senior positions within Australian corporate organisations. In investigating this phenomenon, the research question: *To what extent, if any, does the Australian corporate environment have a career progression ceiling for security practitioners?* was posed.

In response, the findings suggest that there is indeed a security occupational progression ceiling, both in terms of complexity progression as well as hierarchical progression (Freidman et al., 2015). Security roles, even at the strata peak appear to be less complex than higher order executive positions due to the specialised and bounded focus of the work; particularly due to the limited management of uncertainty outside the security domain speciality (Maitland & Sammartino, 2014; Milliken, 1987), as would be expected from technostructure functions. Moreover, in consideration of the discovered security roles along the work strata, the most senior security seatings align most closely with the socio-organisational literatures articulation of general managers and not executive managers (Clement, 2015; Clement & Clement, 2013; Mintzberg, 1980, 2009).

Therefore, it is suggested that the security occupation reaches a progression ceiling at Stratum Four and meets its complexity ceiling at what has been termed tactical work. It would be expected that executive security roles, if uncovered, would transition from tactical work to strategic work; taking on more unstructured and non-domain specific complexity and managing this over a longer time span of discretion than what was found in the current security work hierarchy (Clement & Clement, 2013; Sammarra et al., 2012). They would also transcend security problem solving and tackle broader organisational problems outside of their domain specialty.

Accordingly, security practitioners in the uncovered work hierarchy align with Mumford et al. (2007) and Brooks and Corkill's (2014) discussion of career progression, where as individuals move up in seniority within an organisation, their reliance on general managerial skills increases, and their use of technical skills decreases. The uncovered roles within the security stratum suggest a progression away from technical tasks to generalist tasks within the work stream. Nevertheless, while more senior security roles are more general in nature (i.e. they apply more general skills to their work, such as finance, human resource management, negotiation, and so on), they are still applying these generalist skills to security problems, not broader, general, organisational problems.

With this in mind, the findings included career progression considerations for security practitioners, including their starting point, and overall indicators for success. Such findings prefaced the specialised nature of security work, even at the higher strata roles, and subsequently, led to the postulated progression ceiling (Figure 16).

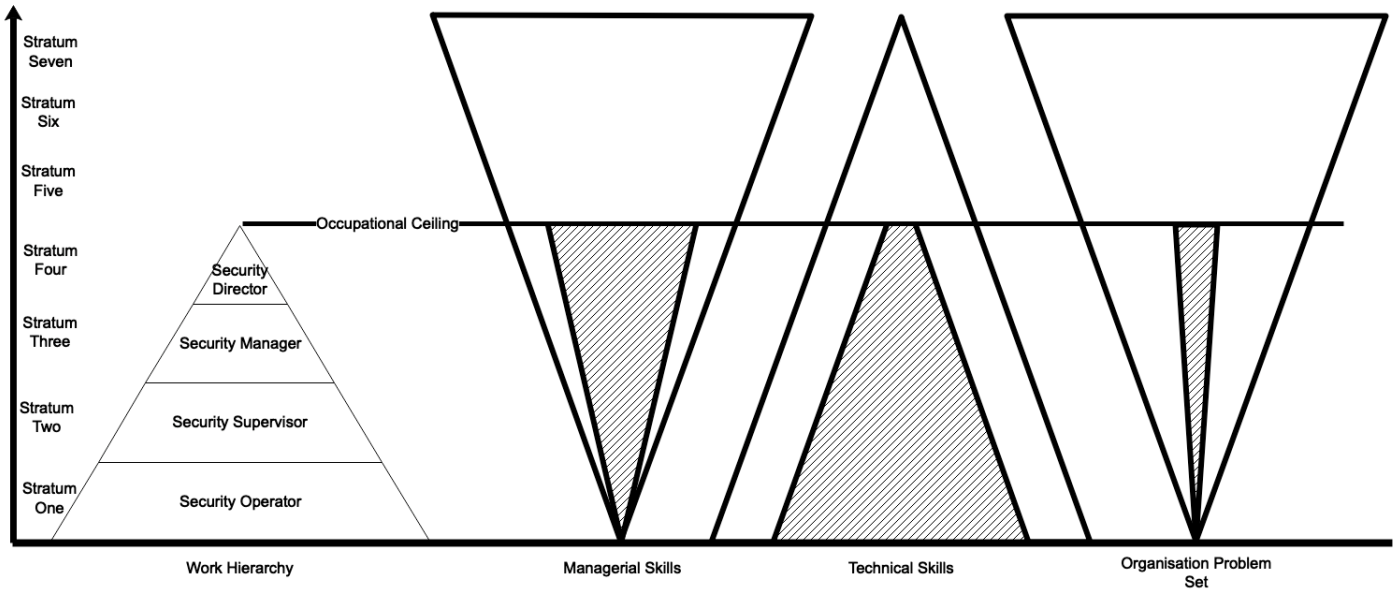

Figure 16. Security Occupation Ceiling

7.3.1 Security as Specialised Work

The career backgrounds uncovered in the study generally suggest a highly specialised workforce within the Corporate Security domain. While senior security professionals were uncovered with titles such as 'Director of Security' and these roles articulated work of a similar nature to executive security roles as articulated by Brooks and Corkill (2014) and McKinley Advisors (2018); those being non-technical security practitioners with responsibility for several organisational functions and long term planning; from a socio-organisational perspective, these uncovered roles are still highly specialised within the security domain (Jaques, 1996).

All participants articulated their work in the context of the specialised practice and implementation of security risk management, with little appreciation for broader decision-making activities outside of their domain. For example, it would be expected that executive managers would discuss their role in broader business activities such as corporate strategy and planning, research and development, public relations, investments and acquisitions, mergers and alliances, marketing, capital expenditure, production and operations, and finance (Sadler-Smith & Shefy, 2004). While the participants were largely silent on these topics, their focus on the influence of security on helping business achieve its objectives and reduce security uncertainty aligns closely with a technostructure role (Ludbey et al.,

2017) which should operate at a lower level of work than executive functions, which is further supported by Maitland and Sammartino (2014).

It is postulated that Corporate Security roles are closely aligned to professional work streams as opposed to managerial work streams as discussed by Sammarra et al. (2012). Professional work streams are those that apply a specific body of knowledge to resolving uncertainty, with a process that does not substantially change between business types. As found, the roles and functions in the Corporate Security work strata are similar in nature, with similar skills, problem solving approaches, and a relatively consistent knowledge base (Coole et al., 2017). Consequently, professional roles would typically be found in technostructure functions and apply their specialised skills to support organisations, but not lead them. Such a view would suggest, as articulated by Sammarra et al. (2012), that career progression for such individuals would be limited if they did not seek opportunities in other organisations to progress; generally, only managerial roles see substantial benefit from remaining in one organisation.

For this reason, it is suggested that Corporate Security roles fulfil an advisory tasking within large organisations at the higher strata of work, but because they do not step outside of their speciality, they remain beneath the executive stream of the organisation. Indeed, while the study found that the higher strata security positions were generally filled by highly educated practitioners wither strong business acumen and managerial skills, their domain specialisation has limited the application of this knowledge within the bounds of security problem solving, limiting opportunity to weigh in on broader business/profit making activities discussion (Bazerman & Moore, 2009).

7.3.2 Occupational Ceiling

Given that there was a tendency for senior staff within the Corporate Security function to have higher education, generally at an undergraduate or master's level, and those in lower strata positions were less educated. The occupational literatures view on the importance of education in career progression within organisations appears to be supported by the findings (McKinley Advisors, 2018; Speer, 2017). In spite of this finding, those in lower strata roles viewed education and training as less useful in career progression, in direct contest to the managerial perspective and the study findings. Several practitioners felt that security education, certification, and other professional development activities were not helpful, even though their managerial team viewed it as essential. This dichotomy of views suggests a miscommunication between strata levels as to expectations for progression within the organisation. Overall, it is suggested that this lack of clear direction and guidance, alongside poor education standards and lack of acceptance for professional certification has substantial impact on promotion and progression pathways (Collins, 1990b; Weeden, 2002). Tied with the perception of

security value and its impact of the broader business results in a limited opportunity for progression and a reduction in strategic impact by practitioners (Oesch, 2015; Speer, 2017).

The study further found that security roles can be limited in opportunities for progression, particularly if individuals do not step outside of a technical security specialisation at some point in their career (Sammarra et al., 2012; Strauss, 1975/2001). Several participants felt they had reached an advancement ceiling within their organisation within the security work hierarchy with lower tier security practitioners finding that lateral moves were not seen as advantageous to their career prospects, and senior security practitioners generally agreeing.

Such limited scope for progression within the occupation is expected due to the specialist nature and lack of alignment with profit-making activities. As Strauss (1975/2001) argues, those practitioners who do not fall within core business roles find progression more difficult, and do not receive the same number of opportunities as their peers. The participants seem to accept and reinforce such a literature viewpoint for security. While Sammarra et al. (2012) suggests that for roles such as those uncovered in this study, progression is most readily achieved by moving between organisations, rather than attempting to climb the progression ladder within the same organisation. In support of this view, one participant explains:

> "looking at my team, they're kind of maxed out, there is nowhere for them to go really...they need a broader set of skills in today's environment at least. There is no way they could go any further."

Subsequently, the study uncovered a security occupational ceiling at the Stratum Four level, which is equivalent to a General Manager position. While it is recognised that some security practitioners achieve role titles such as "Chief Security Officer", and this role is supported by several academic and industry authors (ASIS International., 2004; Cubbage & Brooks, 2013), it is suggested that these role titles are not accurate descriptors of the actual taskings and activities undertaken. Concordant with previous findings from Ludbey et al. (2017), the study found that the specialised nature of the Corporate Security function within corporate organisations does not warrant a seat at the board room table, and is more aligned to other specialised, technostructure roles that feed this specialised knowledge into broader business decision making undertaken by executive staff (Brickley et al., 2009; Sammarra et al., 2012).

The aspiration for Corporate Security to be present at these higher reaches of the organisation is understandable; however, as articulated quite clearly by the organisational literature, such specialised practicing functions are less effective at contributing to unstructured, generalist, and strategic problems faced by those at an executive level of work (Maitland & Sammartino, 2014; Mumford et

al., 2007). This specialisation, paired with the limited exposure career security practitioners have to profit making activities, severely limits opportunity for progression, and overall impact at the strategic level (Speer, 2017). Overall, the findings from this study are supported by the organisational literature and suggest that effective security functions should not seek to operate at the executive level but concentrate on influencing and supporting executive decision making (Papadakis & Barwise, 2002). Furthermore, through an understanding of this hierarchy seating, Corporate Security could leverage its influence towards increasing perceptions of value in the eyes of executive decision makers.

7.4 Conclusion

To sum up, the study uncovered a Corporate Security stratum of work within Australian organisations. The strata of work included Stratum One roles, which implement security controls and respond to security incidents, Stratum Two supervisory roles, which supervise and manage this implementation of security controls within a short time span. Stratum Three managerial roles who interpret the broader security risk management strategy and direct, control, and influence security practitioners in the implementation of this risk management strategy. Finally, the stratum included Stratum Four roles, or general security managers, who set the security direction for the organisation, and create processes and plans to respond to the organisations risk posture as decreed by the executive.

Furthermore, the study found that these four strata positions were oriented according to operational, professional, or tactical functions, each with its own level of influence and authority within organisations (Clarke, 2015). Overall, the security function was found to be a technostructure function due to its technical and specialist body of knowledge that is applied in similar ways across multiple organisations (Sammarra et al., 2012). Furthermore, technostructure roles are those that shape the organisations operating environment through uncertainty and risk management; the security function in this instance manages the security uncertainty and security risk of the organisations operating environment (Bamfield, 2014; Mintzberg, 1980). While those at higher strata security positions do rely on more generalist skills than technical skills, they are still solving specialist security problems and applying their domain specific body of knowledge in their work (Brooks & Corkill, 2014; Maitland & Sammartino, 2014; Mumford et al., 2007).

As a result of this uncovered work strata and the underlying complexity and specialisation of security roles, the study found a career progression ceiling for the occupation. This progression ceiling was at Stratum Four, or a general manager position within organisation. Such a ceiling is not due to education, as most security practitioners at this level were found to be highly educated with strong business acumen (Speer, 2017). Rather, it is postulated that the progression ceiling is due to the strong specialisation of security practitioners at this level of work; their application of general managerial

skills to solve security problems and little input or direction on non-security problems. Overall, specialist technostructure functions like security are not seen at the executive level as they are limited in their capacity to solve problems outside of the deep specialism (Maitland & Sammartino, 2014).

CHAPTER EIGHT

FINDINGS AND CONCLUSION

8.0 Introduction

The Chapter presented the study findings and conclusions, including limitations and recommendations for future research. The study found that there is a significant disconnect between the socio-organisational literature and the security literature when it came occupational stratification, but support for Corporate Security role articulation. The Corporate Security literature supports an executive level Corporate Security practitioner who operates at board level, while the socio-organisational literature supports a middle managerial type role for domain specialists (Bayuk, 2010; Brickley et al., 2009). Whereas the study uncovered a peak Corporate Security seating at Stratum Four (of Seven), which closely aligns to the socio-organisational expectations of a peak Corporate Security role.

Given this uncovered stratum peak, the study also found that Corporate Security progression within organisations is limited to within aligned technical streams, with individuals finding it difficult to progress beyond the specialist stream within organisations (Sammarra et al., 2012). It is posited that the limited interaction and decision making within the bounds of profit-making activities is a contributor to this progression ceiling; security practitioners solve security problems, even at their strata peak, and do not progress to generalist problem solving activities. Subsequently, the occupation's capacity to influence operations laterally across the organisation is limited. While the security occupation is diverse and quite complex, with several competing expectations placed on the roles that make up the security stratum of work, this complexity is bounded wholly within the domain specialty of security and does not transfer to higher order strategic planning or taskings in relation to profit making activities (Le Grand & Tahlin, 2013; Speer, 2017). Overall the study finds that there appears to be an occupational ceiling at the Strum Four (middle management) mark within Australian corporate organisations for Corporate Security practitioners.

8.1 Study Findings

The study found that the Corporate Security stratum of work across four Australian organisations extends across Stratum One through Stratum Four, with Stratum One and Two being operationally and professionally focussed work, and Stratum Three and Four being professionally and tactically focussed work. The study found limited evidence for executive strata roles, even though some participants had executive titles. Further, the study uncovered several security taskings for each strata

position, noting that these findings closely aligned to the security literature (MacCallum, 2013; Sennewald, 2011).

It was considered that the uncovered strata boundary at Stratum Four is related to the capacity of security practitioners to solve organisational problems outside of their specialty. Subsequently it was found that security practitioners, even at higher strata of work, apply managerial skills in security decision making, and remain limited to this area of expertise. In essence, the lack of professionalisation in the industry (Coole et al., 2017; Speer, 2017), paired with the domain specialisation found at the higher reaches of the work hierarchy severely limit the security practitioner from progressing to higher order managerial and executive roles (Maitland & Sammartino, 2014; Papadakis & Barwise, 2002).

Thus, in response to the research question to what extent, if any, does the Australian corporate environment have a career progression ceiling for security professionals? the study intuited that there appears to be a progression ceiling around the Stratum Four position in the work hierarchy. The uncovered progression ceiling is not necessarily related directly to the job title or functional hierarchical position, but rather related to the peak security roles taskings, responsibilities, time span of discretion, and influence.

8.2 Theoretical Implications

The study findings have several implications for the understanding of the Corporate Security function within organisations. These implications include the understanding of Corporate Security careers and their progression in organisations, where the Corporate Security work strata peak is located, and the complexity of security roles. The study findings challenge some security literature assumptions, confirm others, and postulate new research directions for consideration. These outcomes are articulated below.

8.2.1 Corporate Security Careers

While there has been extensive research on occupations, career success, and career progression (Jesus et al., 2015; Sammarra et al., 2012; Speer, 2017; Strauss, 1975/2001; Wrzesniewski et al., 1997), research has often not specifically focussed on security careers (McKinley Advisors, 2018). The study's findings contribute to the literatures understanding of security careers, occupational progression, and professionalisation, noting a conflict in findings with some security literature sources (Bayuk, 2010; Cubbage & Brooks, 2013; Nalla & Morash, 2002).

With reference to the study findings, it was uncovered that security careers progress within their specialist work stream or closely aligned disciplines (such as facility management) with relative ease,

however when attempting to step outside of this function, some difficulty can occur (Strauss, 1975/2001). In contrast however, some participants did enter the security industry from rather disparate backgrounds, still this was not the norm. Overall, it was found that security careers are specialised and remain specialised no matter their hierarchical seating. Security practitioners have opportunities to progress more rapidly by moving between organisations than within it, due to the limited number of roles within organisations and the perceived length of term in senior roles by security practitioners (Jesus et al., 2015; Sammarra et al., 2012).

8.2.2 Corporate Security Role Peak

The study uncovered a peak Corporate Security role, often called the Chief Security Officer in the literature (Cubbage & Brooks, 2013), that is hierarchically seated not at an executive level but at a general managerial level from a complexity and tasking perspective. Such a finding directly challenges the security literature assumptions about the value and influence of the Corporate Security occupation stream. It is premised that the peak security role should organisationally be located at the general managerial level and should not appear in an executive capacity (Jaques, 1996; Jesus et al., 2015; Sammarra et al., 2012). It is argued that the uncovered security executive roles are deep domain specialists with limited general business experience in profit making activities, and thus less suited to c-suite level roles (Maitland & Sammartino, 2014). While they have embraced general managerial traits and activities, they are still bounded within their specialisation when making decisions. Subsequently, those with deep domain specialisation are less capable of making decisions in the face of uncertainty outside of their specified domain, and thus are more suited to managing and operating specialised organisational functions (Clement & Clement, 2013).

Furthering the argument for Corporate Security roles to reach their peak at the general managerial level is the consideration of the uncovered roles time span of discretion (Jaques, 1964). It is suggested that effective and responsive Corporate Security functions need to operate within relatively short time spans of discretion to effectively forecast, plan, and then act on the changing security environment (White, 2014). Such forecasting and planning occurs at the higher levels of work within the function, which was found to be a five-year cycle, firmly placing the peak roles within a tactical time span of discretion in alignment with Jaques (1996) articulation of a Stratum Four role.

Subsequently, it is noted that these findings closely align with the socio-organisational literature, furthering Ludbey and Brooks (2017) and Ludbey et al. (2017) argument that the security literature could be too self-referential, and not adequately considering broader managerial and organisational structural theory. As generally articulated by the socio-organisational literature, specialist functions such as the Corporate Security occupation are limited in their organisational reach, with senior roles

generally tapering off at the middle management level—limiting their lateral power and opportunity to permeate throughout organisations. Furthermore deep domain speciality restricts opportunity for progression, particularly if it is technical specialty not aligned to profit making activities (Heslin, 2005; Speer, 2017; Strauss, 1975/2001). The disparity between the security literature and the broader socio-organisational literature needs to be addressed as it has substantial implications for our understanding of the value, influence, and effectiveness of the security function, particularly as it progresses along a path to professionalisation (McGee, 2006).

8.2.3 Corporate Security Complexity

In contrast to the literature divergence found in the structural significance of the Corporate Security occupation, findings from the study in regard to the complexity of security roles closely aligned to the security literature (Interim Security Professional's Taskforce, 2008; McKinley Advisors, 2018). The findings indicate across all levels of uncovered Corporate Security work a substantial number of responsibilities, not all of which are 'security' roles. For example, participants reported take part in facility management, customer service, and other non-security aligned activities in their role (Brislin, 2014).

Importantly, the complexity of the roles comes from the reactive nature of the function, alongside the difficulties in dealing with people problems; human behaviour can be hard to predict and forecast, leading to substantial uncertainty, particularly over longer time periods (Barefoot & Maxwell, 1987; McCrie, 2001). Furthermore, as discussed by the participants, organisations expect no incidents to occur and when they do, the security team is considered to have failed. Such a high expectation of the function can lead to stress, which is compounded by the multiple sub-roles expected to be fulfilled by security staff, such as customer service, and facility management (Brooks, 2011).

Indeed, the study found security roles in all organisations that aligned strongly with the articulation of Corporate Security in the literature, including security officers, security supervisors, security managers, and security directors (Bamfield, 2014; MacCallum, 2013; Sennewald, 2011). While there was a disparity in these roles position along the work hierarchy, the articulation of their tasks, inputs, and outputs were closely aligned.

8.2.4 Uncovered Assumptions and Limitations of the Security Literature

In review of the theoretical implications, the study has found several underlying assumptions and limitations of the security literature when viewed from a socio-organisational frame. These assumptions and limitations include:

- The Corporate Security literature should seek more direction from the broader socio-organisational and managerial literature when investigating security work hierarchies and role positioning.
- There is an assumption that the security function should be operating at a higher order of work, being functionally seated and positioned at an executive stratum role, the findings of this study suggest that may not be a valid position from the socio-organisational perspective.
- It is possible that the security literature is overemphasising the conduct and implementation of security as being more important and fundamental to organisational success than is the reality. While early managerial authors identified security as a key organisational function (Fayol, 1916/1949), the subsequent lack of conversation in the managerial literature about this work function suggests its value may be limited in consideration of broader business objectives and profit-making activities.

8.3 Industry Implications

The study findings have several implications for industry practitioners and organisations. These implications include the appropriate structure and management of Corporate Security functions, and career directions and strategies for advancement. These outcomes are articulated below.

8.3.1 Corporate Security Work Structure

The study found that the Corporate Security functions investigated had, at times, inconsistent hierarchical seatings by way of time-span of discretion and complexity orientation. For example, several practitioners at a Stratum Three role operating within different levels of complexity, or those with more senior titles having shorter time spans of discretion than those they are managing. Overall, these inconsistencies suggest that these hierarchical structures may be compressed or structurally configured in a less efficient and effective way than may be possible (Ivanov, 2011). Corporate Security work hierarchies should be aligned more closely to the structure articulated by Jaques (1996), where organisation structures are clearly defined by their time span of discretion and problem-solving capacity. It is suggested that Corporate Security functions consider the tasking's provided to subordinates in terms of their time to complete as well as inherent complexity to reduce these cross strata conflicts.

Further evidence of these conflicts arose where managers were found to be interfering with lower strata work tasks. Where work is delegated according to the time span of discretion and complexity of the role, less opportunity and need for this interference (by way of doing the work for the delegee, or micro-managing the individual) would occur (Ivanov, 2015b). Subsequently, Corporate Security managers should carefully define roles and responsibilities, and be cognisant of their subordinate's capacity and capability to undertake the work requested to ensure maximal efficiency in the conduct of security work within the organisation.

Following this, and in alignment with the argument that Corporate Security should not be an executive strata position; it is suggested that peak security roles should embrace specialist knowledge in an applied managerial context and be seen as an advisor and influencer, not decision maker and executive. Security practitioners should be seeking to influence the strategic apex of organisations from a position of specialist expertise that can only be sought by highly valued, but non-career managerial staff; being trusted advisors with a mandate from the executive, not organisational decision makers.

8.3.2 Corporate Security Careers

As found, if security practitioners are finding a career ceiling at the middle management position, career progression may need to be sought through other means. Generally, career managers progress throughout an organisation to the executive seating, particularly when their career aligns with profit making activities (Strauss, 1975/2001). Where individuals are not on the managerial progression track due to their inherent specialisation (as found in technostructure roles), alternative approaches such as moving between organisations should be considered, particularly where some level of occupational closure exists (Weeden, 2002). Where specialists with a distinct body of knowledge that is transferrable between contextual applications (such as different markets, organisations, environments etc), their value to an organisation is in the provision of such expertise to solve organisational problems that suit their speciality. Those within an organisation in a managerial promotion track demonstrate value to the organisation through their strong inter-company relationships, knowledge of the organisation's history and past mistakes, and their products and services (Koch et al., 2015; Sammarra et al., 2012).

With this in mind, Corporate Security practitioners, proposed as technostructure professionals, have their own developing body of knowledge that is applicable no matter the contextual application (Coole et al., 2017; Coole, Brooks, & Treagust, 2015). Subsequently they are more aligned to progress according to specialist means as opposed to managerial means due to their inherent worth to an organisation. Thus, Corporate Security practitioners would likely find more success in career progression, salary increases, and overall standing and influence by moving between organisations over time as opposed to remaining with one over the course of their career (Sammarra et al., 2012).

8.4 Limitations

Some limitations were considered in the study and are presented below. These limitations include the applicability of the underlying theory in modern work environments, the methodological approach, and sample size. Overall, it is expected that these limitations did not substantially impact the findings of the study, but nevertheless are reviewed for completeness.

8.4.1 Underlying Theory

The analysis drew heavily from the underlying theory presented by Jaques (1996), which discusses a key metric in work as the time-span of discretion. This measurement relies on charting an individual's capacity to forecast work into the future and consider first, second, and possibly third order consequences across periods of time. In review, substantial changes in the conduct of work have occurred over the last few decades, with globalisation and technology increasing the pace of business (Boal & Whitehead, 1992; Ivanov, 2006; Rossi, 2008; Stichweh, 2008). Such changes may influence the applicability of the time span of discretion metric in modern work.

However, Clement (2015), and Ivanov (2015a) still support a modern application of Jaques' general theory of organisational structure (1996). They do comment on the compression of work in modern organisations, but Ivanov (2011) points to this not as a result of modern working conditions, but towards fundamental decisions about structural make up that results in failed organisations. Subsequently, while it is possible that the modern work hierarchy is by its very nature compressed as a matter of course, it is unlikely that the metric of time span of discretion is no longer valid for identifying individuals' level of work and capacity to fulfil taskings within each stratum (Clement & Clement, 2013).

8.4.2 Methodology

In review of the methodology, some limitations were noted in this study. While the two-phase approach provided significant validity and reliability to the findings, the limited sample size for Phase One and Two limits the generalisability of the findings (Collier & Elman, 2008). This limitation is particularly true for the limited number of participatory organisations (four in Phase One, three in Phase Two). Gaining access to the security functions within more large Australian organisations would have provided further confidence in the results.

Furthermore, consideration to the first phase instrument is given. While the instrument was developed and tested in previous research (Ludbey, 2016), some inconsistency was found between the sub-instruments. For example, the Work Measurement Scale showed limited correlation to the Task Complexity Measurement Tool. Further investigation into this tool's reliability is required, however for the purposes of this study, the appropriate level of correlation was found when considering the whole sample across all organisations. The noted correlation limitations may only be present in smaller sample sizes as used in this study (Witte & Witte, 2017).

8.4.3 Data Collection

There were some limitations in the data collected which influences the applicability of the study findings to the broader population of Corporate Security practitioners. Phase One's survey sample was relatively small, even though three of the four organisations had a response rate of over 10% of their security function (Fowler, 2014). Considering the size of these internal security functions in relation to the broader security community, the response rate for this Phase is not directly attributable to the industry at large. Further, the Phase Two interviews and focus groups were extensive for three of the four organisations, however the research was unable to get interview participants from one of the four organisations, limiting the cross-comparison between Phase findings.

Nevertheless, the varied, two phase methodology, alongside the careful selection of participating organisations and their distinct market segments provided some affirmation that the data collection, while limited in sample size, holds validity (Witte & Witte, 2017). The interview and focus groups were detailed and data-rich, which was supported by extensive analysis. Further, the phase findings did support each other, lending credence to the reliability of the findings.

8.5 Recommendations

The study presents significant findings toward understanding the structure, influence, and value of the Corporate Security function within large organisations. Admittedly, there are some limitations to the study, such as sample size, however the implications of the uncovered findings are in alignment with previous research, lending validity (Ludbey et al., 2017). Subsequently, a series of recommendations are made in considering future research directions:

- The study postulated one of the reasons for the uncovered security progression ceiling due to the executive staff not delegating or defining the appropriate responsibilities for these positions. Where the roles are not appropriate defined, and tasks not appropriately delegated, those being recruited to fulfil those roles will not be of an appropriate seniority. Nevertheless, the study did not explore this possibility in detail due to restrictions in methodology and participants, and this research avenue should be continued in future study;
- The study only observed large Australian enterprises and did not seek participants from small to medium enterprises. It is possible that the security stratum of work differs for different organisation sizes and this should be reviewed in future studies;
- While the study was oriented towards the Australian context, replicating the chosen methodology to investigate international security functions would provide further evidence towards the applicability of these findings to Corporate Security as a whole;
- The identified disconnect between the Corporate Security literature and the broader socio-organisational literature should be addressed through further research. Where this study has uncovered some underlying assumptions and limitations of the security literature, a more rigorous investigation is required;

- More research into the careers within the Corporate Security function are required, and should be grounded in the extensive career literature, and not the security literature. For example, an analysis of security career orientations in concordance with the conceptualisation of career anchors, boundaryless and protean careers and other such underlying factors would be useful in determining the true scope of the security occupation.

8.6 Conclusion

To conclude, Corporate Security is a growing and significant industry and occupation in Australia, with increasing expectations to reduce security uncertainty and security risk; enabling organisations to operate effectively (Brooks & Smith, 2012). In part, these expectations stem from corporate social responsibilities as opposed to profit-making imperatives (Petersen, 2013). It is postulated that these growing expectations align with the modern interpretation of risk and the societal expectations around managing all foreseeable risk (Beck, 1992). Nevertheless, Corporate Security does play a role in developing business resilience in the face of security threats and disruptive circumstances, which ultimately support profit-making indirectly.

Such indirect support of profit-making includes interfaces between organisational decision makers and the operating environment for the business. Corporate Security is responsible for identifying, assessing, and managing potential security threats and risks in support of the broader business strategies as set and directed by the executive strata (Coole et al., 2017; Ludbey et al., 2017). Subsequently, the Corporate Security technostructure function needs to be responsive to emerging threats and risks and interpret the operating environment into actionable intelligence for executive decision makers. This role within the organisation is a specialised one, and as such, this specialisation influences opportunities for career progression (Strauss, 1975/2011).

Corporate role progression, particularly into the upper echelons of management, is usually more favourable to generalist problem solvers who are aligned to profit-making activities (Holland et al., 2012, pp. 122-134). As Corporate Security roles are specialised, and while more senior security practitioners apply generalist managerial skills to their work, they are not solving broader and general profit-making or business problems, they are solving security problems. Thus, the study found an occupation ceiling at the general manager position (Stratum Four) which aligns with the expected peak for specialist technostructure roles. Consequently, it is argued that while progression within such a specialised hierarchy is difficult due to the inherent specialisation of the roles fulfilled, opportunities for career progression would exist outside of the organisation of current employment and moving between organisations would likely lead to improved salary and benefits over time (Sammarra et al., 2012).

Finally, it is acknowledged that Corporate Security plays an important role in risk mitigation for organisations, and that the roles and responsibilities of the function are increasing as the occupation becomes more accepted (Bergin et al., 2018). Nevertheless, it is argued that the Corporate Security Function is indeed positioned correctly within organisations in its current form, and the market has decided where Corporate Security roles fit due to societal forces and the organisational value

generated by such roles. While Corporate Security adds value from a specialist perspective; supporting business decisions and being a trusted advisor, this value is not sufficient enough to elevate the function to a senior executive seating as the norm.

The findings from the study emphasise a new model of security work within organisations to explain these occupational ceilings and progression opportunities. This model describes corporate security not as an executive function, but as a general managerial one. Within this general managerial work hierarchy, security operatives are specialised within the domain of security problem solving, and thus lack a broader view of organisational decision making. Subsequently, corporate security is not responsible for strategic direction at the organisational peak but interprets and is directed by this peak to implement security measures at all organisational levels to support profit making activity and other corporate social responsibility objectives (Petersen, 2013).

Moreover, the study challenges two key approaches in the corporate security literature that need to be addressed through future research. Firstly, the literature rarely draws from the broader socio-organisational and managerial literature when investigating security work hierarchies and roles positioning. While the study confirms the articulation of security roles (tasks and activities), it contests the literatures understanding of how these roles interoperate within an organisation from a structural perspective. It is postulated that this is due to the limited number of studies taking an 'outside in' approach—it is common for security research to be undertaken from within the discipline and corresponding literature (Ludbey et al., 2017). Secondly, and possibly due to this preceding point, the literature posits an executive level position for security practitioners which the socio-organisational literature and the findings of this study contend. Corporate security, while at the hierarchical peak is general in the day to day tasks, is still highly specialised within one problem-solving domain. Such limitations in the occupation's domain problem solving capacity severely limit opportunity within the executive stream (Holland et al., 2012, pp. 122-134).

While it is expected that executive level security practitioners do exist, it is postulated that these practitioners are really fulfilling a general managerial tasking and have been seated inappropriately within the organisation. Future investigation should consider the tasks these executive practitioners fulfil when uncovered within the broader organisational purview before a conclusion about the appropriateness of security in the executive is made.

REFERENCE LIST

Abbott, A. D. (1988). *The System of Professions an Essay on the Division of Expert Labor*. Chicago: University of Chicago Press.

Allison, D. J., & Morfitt, G. (1994). *Time span of discretion and administrative work in school systems: results of a pilot study*. Paper presented at the The Annual Meeting of the American Educational Research Association, New Orleans. http://files.eric.ed.gov/fulltext/ED374530.pdf

Allison, D. J., Morfitt, G., & Demaerschalk, D. (1996). *Cognitive complexity and expertise: relationships between external and internal measure of cognitive complexity and abstraction, and responses to a case problem*. Paper presented at the The Annual Meeting of the American Educational Research Association, New York City. http://files.eric.ed.gov/fulltext/ED412604.pdf

Andersen, T., Garvey, M., & Roggi, O. (2014). Risk, Risk Management, and Risk Governance *Managing Risk and Opportunity: The Governance of Strategic Risk-Taking.* Oxford: Oxford University Press.

Apollo Education Group. (2015). *Operational Security Industry Competency Model*. ASIS International. Phoenix: University of Phoenix.

ASIS International. (2004). *Chief Security Officer Guideline*. Retrieved from: https://cdn.fedweb.org/137/268/ASIS%2520Chief%2520Security%2520Officer%2520Guide-Public.pdf

Australian Security Industry Association Limited. (2017). *Research and Statistics.* Retrieved from https://www.asial.com.au/resources/research-and-statistics

Baker, P. R., & Benny, D. J. (2013). *The Complete Guide to Physical Security*. Boca Raton, FL: Taylor & Francis Group, LLC.

Bamfield, J. (2014). Security and Risk Management. In Gill (Ed.), *The Handbook of Security* (2nd ed., pp. 791-812). Hampshire: Palgrave Macmillan.

Barefoot, J. K., & Maxwell, D. A. (1987). *Corporate Security Administration and Management*. Boston: Butterworth Publishers.

Barkema, H. G., Baum, J. A. C., & Mannix, E. A. (2002). Management challenges in a new time. *The Academy of Management Journal, 45*(5), 916-930.

Barnard, C. I. (1938/1971). *The Functions of the Executive*. Cambridge, MA: Harvard University Printing Office.

Bayuk, J. L. (2010). *Enterprise Security for the Executive*. Santa Barbara, California: Praeger.

Bazerman, M. H., & Moore, D. A. (2009). *Judgement in Managerial Decision Making*. MA: John Wiley & Sons, Inc.

Beck, U. (1992). *Risk Society Towards a New Modernity* (M. Ritter, Trans.). Thousand Oaks, CA: SAGE Publications Ltd.

Bergin, A., Williams, D., & Dixon, C. (2018). *Safety in Numbers Australia's Private Security Guard Force and Counterterrorism*. Canberra: Australian Strategic Policy Institute.

Bilgin, P. (2003). Individual and societal dimensions of security. *International Studies Review, 5*, 203-222.

Black, C. (2004). The security of business: a view from the security industry. In A. Bailes, J. K., & I. Frommelt (Eds.), *Business and Security*. New York: Oxford University Press.

Bloor, M., Frankland, J., Thomas, M., & Robson, K. (2001). *Focus Groups in Social Research* (M. Thomas Ed.). London: SAGE Publications Ltd.

Boal, K. B., & Whitehead, C. J. (1992). A Critique and Extension of the Stratified Systems Theory Perspective *Strategic Leadership A Multiorganizational-Level Perspective*. Westport, CT: Quorum Books.

Brandtnera, P., Helfertb, M., Auingera, A., & Gaubingera, K. (2015). Conducting focus group research in a design science project: Application in developing a process model for the front end of innovation. *Systems, Signs & Actions, 9*(1), 26-55.

Brannick, M., T.,, & Levine, E., L. (2002). *Job Analysis*. Thousand Oaks, California: SAGE Publications, Inc.

Braun , V., & Clarke, V. (2008). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2).

Brickley, J., A.,, Smith, C., W.,, & Zimmerman, J., L. (2009). *Managerial economics and organizational architecture* (5th ed.). New York, NY: McGraw-Hill/Irwin.

Brislin, R. (2014). *The Effective Security Officers Training Manual* (3rd ed.). Waltham, MA: Elsevier Inc.

Brock, D. (2008). Hotel security and the routine activites approach. *Police journal, 81*(2), 144.

Brooks, D. (2011). Security risk management: A psychometric map of expert knowledge structure. *Risk Management, 13*(1-2), 17-41.

Brooks, D. (2013). Corporate security: using knowledge construction to define a practising body of knowledge. *Asian Journal of Criminology, 8*(2), 89-101.

Brooks, D. (2014). Intrusion Detection Systems in the Protection of Assets. In Gill (Ed.), *The Handbook of Security* (2nd ed., pp. 683-704). Hampshire: Palgrave Macmillan.

Brooks, D., & Coole, M. P. (2017). Codifying knowledge in the development of the discipline of security science: knowledge to diagnose, infer and treat the security problem. *The 2nd International Conference on Engineering Sciences and Technologies*. doi:10.1201/9781315210469-309

Brooks, D., & Corkill, J. (2014). Corporate Security and the Stratum of Security Management *Corporate Security in the 21st Century : Theory and Practice in International Perspective* (1st ed., pp. 216-234): Palgrave Macmillan.

Brooks, D., & Smith, C. (2012). *Security Science : The Theory and Practice of Security* Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=1106489

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford: Oxford University Press.

Burnstein, H. (1978). Beyond cops and robbers: a note on corporate security. *University of Michigan Business Review*, 30-32.

Christensen, L., & Johnson, R. B. (2014). *Educational Research Quantitative, Qualitative and Mixed Approaches* (5th ed.). London: SAGE Publications.

Clarke, T. (2015). Changing paradigms in corporate governance: new cycles and new responsibilities. *Society and Business Review, 10*(3), 306-326.

Clement, S. D. (2015). Time-span and time compression: New challenges facing contemporary leaders *Journal of Leadership and Management, 2*(4), 35-40.

Clement, S. D., & Clement, C. R. (2013). *All About Work*. The Woodlands, TX: Organizational Design Inc.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). New York: Routledge.

Collier, D., & Elman, C. (2008). Qualitative and multi-method research: Organizations, publication, and reflections on integration *The Oxford Handbook of Political Methodology*. Oxford: Oxford Universty Press.

Collins, R. (1990a). Changing Conceptions in the Sociology of the Professions. In R. Torstendahl & M. Burrage (Eds.), *The Formation of Professions* (pp. 11-23). London: SAGE Publications Inc.

Collins, R. (1990b). *Market Closure and the Conflict Theory of the Professions* (M. Burrage & R. Torstendahl Eds.). London: SAGE Publications Ltd.

Coole, M. P., Brooks, D., & Minnaar, A. (2017). The physical security professional: Mapping a body of knowledge. *Security Journal, 30*(4), 1169-1197.

Coole, M. P., Brooks, D., & Treagust, D. (2015). The physical security professional: formulating a novel body of knowledge. *Journal of Applied Security Research, 10*(3), 385-410.

Craddock, K. (2002). Requisite leadership theory: an annotated research bibliography on elliott jaques, including: requisite organization - the glacier project - stratified systems theory - time-span of discretion - levels of mental complexity - complexity of information processing - the quality of labor - the mid-life crisis - and psychoanalysis (covering 1942-2002). Columbia University.

Craighead, G. (2009). *High-Rise Security and Fire Life Safety* (3rd ed.). Oxford: Butterworth-Heinemann.

Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). New Delhi: SAGE Publications India Pvt Ltd.

Cubbage, C., & Brooks, D. (2013). *Corporate Security in the Asia-Pacific Region*. Boca Raton, FL: CRC Press, 2013.

Dadashi, N., Stedmon, A. W., & Pridmore, T. P. (2013). Semi-automoated CCTV surveillence: the effects of system confidence, system accuracy and task complexity on operator vigilance, reliance and workload. *Applied Ergonomics, 44*(5), 730-738.

Dahrendorf, R. (1959). Class and Class Conflict in Industrial Society Retrieved from: http://solomon.sth2.alexanderstreet.com.ezproxy.ecu.edu.au/cgi-bin/asp/philo/sth2/documentidx.pl?sourceid=S10021368

Davis, K., & Moore, W. E. (1945). Some Principles of Stratification. *American Sociological Review, 10*(2), 242-249.

Deming, E., W. (2013). *The Essential Deming: Leadership Principles from the Father of Quality*. New York: McGraw Hill.

Denzin, N. K. (1989). *The research act: a theoretical introduction to sociological methods* (3rd ed.). Englewood Cliffs, NJ: Prentice-Hall.

Dillon, M. (2013). *Introduction to Sociological Theory : Theorists, Concepts, and their Applicability to the Twenty-First Century* Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=1566387

Donald, F. M. (2010). A model of CCTV surveillance operator performance. *Ergononmics SA, 22*(2), 2-13.

Dubow, E. F., Boxer, P., & Huesmann, L. R. (2009). Long-term effects of parents' education on children's educational and occupational success: mediation by family interactions, child aggression, and teenage aspirations. *Merrill-Palmer Quarterly (Wayne State University. Press), 55*(3), 224-249.

Durkheim, E. (1893/1984). *The Division Of Labour In Society* (W. D. Halls, Trans.). Basingstoke: Macmillan.

Durkheim, E. (1993). *The Division Of Labour In Society*. Glencoe, IL: Free Press.

Elenkov, D. S. (1997). Strategic uncertainty and environmental scanning: the case for institutional influences on scanning behavior. *Strategic management journal, 18*(4), 287-302.

Farquhar, J. D. (2012). *Case Study Research for Business* London: SAGE Publications Ltd.

Fay, J. J. (2002). *Contemporary Security Management*. Burlington, MA: Butterworth-Heinemann.

Fayol, H. (1916/1949). *General and Industrial Management*. Chicago: Pitman Publishing Corporation.

Field, A. (2013). *Discovering Statistics using IBM SPSS Statistics* (M. Carmichael Ed. 4th ed.). Thousand Oaks, CA: SAGE Publications Ltd.

Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to Security* (8th ed.). Oxford: Butterworth-Heinemann.

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk *Policy Sciences, 17*, 123-139.

Fowler, F. J. (2014). *Survey Research Methods* (5th ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Freeman, D., & Freeman, J. (2008). *Paranoia the 21st-Century Fear*. New York: Oxford University Press.

Freidman, S., Laurison, D., & Miles, A. (2015). Breaking the 'class' ceiling?: social mobility into Britain's elite occupations. *The Sociological Review, 63*(2), 259-289.

Friedman, M. (2002). *Capitalism and Freedom*. London: The University of Chicago Press.

Friedson. (1984). Are Professions Necessary? In H. J. Graff (Ed.), *The Authority of Experts*. Indiana: Indiana University Press.

Galbraith, J. K. (1985). *The New Industrial State* (4th ed.). Boston: Houghton Mifflin Company.

Gill, M. (2014). Exploring Some Contradictions of Modern-Day Security. In Gill (Ed.), *The Handbook of Security* (2nd ed., pp. 980-1000). Hampshire: Palgrave Macmillan.

Gill, M., & Howell, C. (2012). *The security sector in perspective*. Retrieved from: *http://www.mocotouch.co.uk/library/2012-08_The_security_sector_in_perspective.pdf*

Gill, M., & Howell, C. (2014). Policing organisations: the role of the corporate security function and the implications for suppliers. *International Journal of Police Science & Management, 16*(1), 65-75.

Gill, M., Taylor, E., Bourne, T., & Keats, G. (2008). *Organisational Perspectives on the value of Security* Retrieved from: http://www.perpetuityresearch.com/images/Reports/2008%20SRI%20-%20Organisational%20perspectives%20on%20the%20value%20of%20security.pdf

Gill, P., & Pythian, M. (2006). *Intelligence in an Insecure World*. Cambridge: Polity Press.

Greene, J., & D'Oliveira, M. (2005). *Learning to Use Statistical Tests in Psychology*. Maidenhead: McGraw-Hill Education.

Grobler, S. W. (2005). *Organisational Structure and Elliot Jaques' Stratified Systems Theory.* (Masters Degree in Business Leadership), University of South Africa, South Africa.

Grusky, D. B., & Sorenson, J. B. (1998). Can class analysis be salvaged? *American Journal of Sociology, 103*(5), 1187-1234.

Gyarmati, I. (2004). Security and the responsibilities of the public and private sectors. In J. K. A. Bailes & I. Frommelt (Eds.), *Business and Security*. New York: Oxford University Press.

Hasan, A. (2016). Security of cross-country oil and gas pipelines: a risk-based model. *Journal of Pipeline Systems Engineering and Practice, 7*(3), 04016006-1-04016006-8.

Hausman , D., M.,. (1989). Economic methodology in a nutshell. *Journal of Economic Perspectives, 3*(2), 115-127.

Hayes, R. (2003). Loss prevention: senior management views on current trends and issues. *Security Journal, 16*(2), 7-20.

Heath, A. (1981). *Social Mobility*. London: Fontana Paperbacks.

Heslin, P., A.,. (2005). Conceptualizing and evaluating career success. *Journal of Organizational Behaviour, 26*(2), 113-136.

Hintze, J. L., & Nelson, R. D. (1998). Violin plots: a box plot-density trace synergism. *The American Statistician, 52*(2), 181-184.

Holland, P., Sheehan, C., Donohue, R., Pyman, A., & Allen, B. (2012). *Contemporary Issue and Challenges in HRM*. Prahran, VIC: The Tilde Group.

IFPO. (2008). *Security Supervision and Management: The Theory and Practice of Asset Protection* (3rd ed.). Oxford, UK: Elsevier Science.

Interim Security Professional's Taskforce. (2008). *Advancing Security Professionals*. Retrieved from http://www.isacaadelaide.org/pd/Discusion_paper_Future_Security_Professionals_March08.pdf.

Ivanov, S. (2006). *Investigating the optimum manager-subordinate relationship of a discontinuity theory of managerial organisations: an exploratory study of a general theory of managerial hierarchy.* (Doctor of Philosophy), The George Washington University, Washington DC. Retrieved from https://sergeyivanovorg.sharepoint.com/Documents/Sergey_Ivanov_PhD_PUBLIC_2014_12_01.pdf

Ivanov, S. (2011). Why organizations fail: a conversation about American competitiveness. *International Journal of Organizational Innovation, 4*(1).

Ivanov, S. (2015a). Exposing myths of modern management: Innovation – identifying the problem. *Journal of Leadership and Management, 1*(2015), 57-66.

Ivanov, S. (Producer). (2015b, 16 January 2018). Innovation, Ethics, Morality. [Recorded Academic Lecture] Retrieved from https://www.youtube.com/watch?v=7B1GqogYvik

Jacobs, O. T., & Lewis, P. (1992). Leadership requirements in stratified systems *Strategic Leadership A Multiorganizational-Level Perspective*. Westport, CT: Quorum Books.

Jaques, E. (1951). *The Changing Culture of a Factory a Study of Authority and Participation in an Industrial Setting*. London: Tavistock Publications Limited.

Jaques, E. (1964). *Time-Span Handbook How to use time-span of discretion to measure the level of work in employment roles and to arrange an equitable payment structure*. London: Heinemann Educational Books Ltd.

Jaques, E. (1976). *A GeneralTtheory of Bureaucracy.* London: Heinemann Educational Books Ltd.

Jaques, E. (1986). The development of intellectual capability: a discussion of stratified systems theory. *The Journal of Applied Behavioral Science, 22*(4), 361-383.

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

Jaques, E. (2002). *The Life and Behavior of Living Organisms A General Theory*. Westport: CT: Praeger Publishers.

Jesus, B., Seibert, S. E., Kraimer, M., Wayne, S., & Liden, R. (2015). Measuring career orientations in the era of the boundaryless career. *Journal of Career Assessment, 25*(10), 502-525.

Jo, T., H. (2018). The Institutionalist Theory of the Business Enterprise: Past, Present, and Future. *Munich Personal RePEc Archive*.

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review, 31*(2), 386-408.

Koch, M., Forgues, B., & Monties, V. (2015). The way to the top: career patterns of fortune 100 CEOs. *Human Resource Management, 52*(2), 267-285.

Krahman, E. (2008). Security: collective good or commodity? *European Journal of International Relations, 14*(3), 379-404.

Krugman, P., & Wells, R. (2006). *Economics*. New York: Worth Publishers.

Laerd Statistcs. (2013). *Spearman's Rank-Order Correlation*. Retrieved from https://statistics.laerd.com/statistical-guides/spearmans-rank-order-correlation-statistical-guide.php

Laner, S., & Crossman, E. R. F. W. (1976). The Current Status of the Jaquesian Time-Span of Discretition Concept: Research and Applications. In J. L. Gray (Ed.), *The Glacier Project: Concepts and Critiques* (pp. 201-226). London: Heinemann Educational Books Ltd.

Laner, S., Crossman, E. R. F. W., & Baker, H. T. (1969). *Measurement of Responsibility: A Critical Evaluation of Level of Work Measurement by Time-Span of Discretion* (HFT-69-10). Retrieved from Berkeley: http://files.eric.ed.gov/fulltext/ED045717.pdf

Lawler III, E. E., & Rhode, J. G. (1976). *Information and Control in Organizations*. California: Goodyear Publishing Company, Inc.

Lazear, E., P. (2000). Economic imperialism. *Quarterly Journal of Economics, 115*(1), 99-146.

Le Grand, C., & Tahlin, M. (2013). Class, Occupation, Wages, and Skills: The Iron Law of Labor Market Inequality. In E. B. Gunn (Ed.), *Class and Stratification Analysis*. Bingley, UK: Emerald Group Publishing Ltd.

Leonard-Barton, D. (1990). A dual methodology for case studies: synergistic use of a longitudinal single site with replicated multiple sites. *Organization Science, 1*(3), 248-266.

Lippert, R., K.,, & Walby, K. (2014). Critiques of Corporate Security: Cost, Camouflage and Creep. In Gill (Ed.), *The Handbook of Security* (2nd ed., pp. 881-900). Hampshire: Palgrave Macmillan.

Litterer, J. A. (1963). *Organizations: Structured Behaviour*. New York: John Wiley and Sons.

Loveday, K., & Gill, M. (2004). The impact of monitored cctv in a retail environment: what cctv operators do and why. *Crime Prevention and Community Safety, 6*(3), 43-55.

Lucier, J. P. (1999). Nuclear security. *Insight on the News, 15,* 10-11.

Ludbey, C. (2016). *The Corporate Security Stratum of Work: Identifying Levels of Work in the Domain.* (Bachelor of Science (Security) Honours), Edith Cowan University, Perth, WA. Retrieved from http://ro.ecu.edu.au/theses_hons/1489

Ludbey, C., & Brooks, D. (2017). Stratum of security practice: using risk as a measure in the stratification of security works. *Security Journal 30*(3), 686-702.

Ludbey, C., Brooks, D., & Coole, M. P. (2017). Corporate security: identifying and understanding the levels of security work in an organisation. *Asian Journal of Criminology*, *13*(2), 109-128.

MacCallum, W. (2013). *Governance of Security Systems A Handbook for Designing and Implementing a Security Program That Will Protect Your Business*. Canberra: Collaborative Publications.

Mahajan, J. P. (2010). *Business Organisation and Management*. Mumbai: Himalaya Publishing House.

Maitland, E., & Sammartino, A. (2014). Decision-making and uncertainty: The role of heuristics and experience in assessing a politcally hazardous environment. *Strategic management journal, 36*(10), 1554–1578.

Manunta, G. (1996). The case against: security management is not a profession. *International Journal Of Risk, Security And Crime Prevention, 1*(3), 233-240.

Marcuse, P. (2006). Security or safety in cities? The threat of terrorism after 9/11. *International Jounral of Urban and Regional Research, 30*(4), 919-929.

Marquette, H., & Peiffer, C. (2015). *Corruption and Collective Action*. Retrieved from: http://publications.dlprog.org/CorruptionandCollectiveAction.pdf

Marsden, D. (1999). *A Theory of Employment Systems*. New York: Oxford University Press.

Marx, K., & Engels, F. (1848/1963). *The Communist Manifesto* D. Ryzanoff (Ed.)

McCrie, R. D. (2001). *Security Operations Management*. Woburn: Butterworth-Heinemann.

McGee, A. (2006). *Corporate Security's Professional Project: An Examination of the Modern Condition of Corporate Security Management, and the Potential for Further Professionalisation of the Occupation.* (Master of Science (by research)), Cranfield University, Cranfield.

McGregor, C. (1997). *Class in Australia*. Ringwood, Victoria: Penguin Books Australia Ltd.

McKinley Advisors. (2018). *Security Industry Career Pathways Guide Practitioners and Suppliers*. Retrieved from: https://www.asisonline.org/globalassets/professional-development/careers/documents/careerpathwaysguide.pdf

McMorland, J. (2005). Are you big enough for your job? Is your job big enough for you? Exploring levels of work in organisations. *University of Auckland Business Review*. Retrieved from http://dmcodyssey.org/wp-content/uploads/2013/08/BigEnoughForJob_MacMorland.pdf

Merriam, S. B. (2009). *Qualitative Research A Guide to Design and Implementation*. Somerset: Wiley.

Mill, J. S. (1869). *On Liberty* (4th ed.). London: Longman, Roberts & Green.

Milliken, F. J. (1987). Three types of perceived uncertainty about the environment: state, effect, and response uncertainty *Academy of Management Review, 12*(1).

Mintzberg, H. (1979). *The Structuring of Organizations*. New Jersey: Prentice-Hall Inc.

Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. *Management Science, 26*(3), 322-341.

Mintzberg, H. (1989). *Mintzberg on Management*. New York, NY: The Free Press.

Mintzberg, H. (2009). *Managing*. California: Berrett-Koehler Publishers Inc.

Molotch, H., & Molotch, H. (2012). *Against Security : How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*. Princeton: Princeton University Press.

Morgan, D. L. (1997). *Qualitative Research Methods: Focus Groups As Qualitative Research*. London: SAGE Publicatins Ltd.

Mumford, T. V., Campion, M. A., & Morgeson, F. P. (2007). The leadership skills strataplex: Leadership skill requirements across organizational levels. *The Leadership Quarterly, 18*(2), 154-166.

Murphy, R. (1990). Proletarianization or bureaucratization: the fall of the professional? In R. Torstendahl & M. Burrage (Eds.), *The Formation of Professions* (pp. 71-96). London: SAGE Publications Inc.

Nalla, M., K., Johnson, J., & Mesko, G. (2009). Are police and security personnel warming up to each other? A comparison of officers' attitudes in developed, emerging, and transitional economies. *Policing: An International Journal of Police Strategies and Management, 32*(3), 508-552.

Nalla, M., K., & Morash, M. (2002). Assessing the scope of corporate security: common practices and relationships with other business functions. *Security Journal, 15*(3), 7-19. d

Nalla, M., K., & Wakefield, A. (2014). The security officer. In Gill (Ed.), *The Handbook of Security* (2nd ed., pp. 727-746). Hampshire: Palgrave Macmillan.

Neocleous, M. (2000). Against security. *Radical Philosophy, 100*, 7-15.

Neocleous, M. (2006). The problem with normality: taking exception to "permanent emergency". *Alternatives, 31*, 191–213.

Neocleous, M. (2007). Security, liberty and the myth of balance: towards a critique of security politics. *Contemporary Political Theory, 6*, 131–149.

Ocqueteau, F. (2012). Heads of corporate security in the era of global security *Champ pénal/Penal field [En ligne], 8*. doi:10.4000/champpenal.8245

Oesch, D. (2015). Occupational structure and labor market change in Western Europe since 1990. In P. Beramendi, Häusermann, S, Kitschelt, H, Kriesi, H (Ed.), *The Politics of Advanced Capitalism* (pp. 112-132). Cambridge, UK: Cambridge University Press.

Papadakis, V. M., & Barwise, P. (2002). How much do CEOs and top managers matter in strategic decision-making? *British Journal of Management, 31*(1), 83-95.

Papadakis, V. M., Lioukas, S., & Chambers, D. (1998). Strategic decision-making processes: the role of managment and context. *Strategic management journal, 19*(2), 115-147.

Parsons, T. (1951). *The Social System*. London: Routledge.

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory And Practice* (4th ed.). Thousand Oaks, California: SAGE Publications, Inc.

Petersen, K. L. (2013). *The Corporate Security professional: a hybrid agent between corporate and national security*. Paper presented at the International Studies Association Annual Convention, San Francisco.

Petersen, K. L. (2014). The politics of corporate security and the translation of national security. In Walby K. & L. R.K. (Eds.), *Corporate Security in the 21st Century. Crime Prevention and Security Management*. London: Palgrave Macmillan.

Prenzler, T. (2005). Mapping the australian security industry. *Security Journal, 18*(4), 51-64.

Prenzler, T., Earle, K., & Sarre, R. (2009). Private security in Australia: trends and key characteristics. *Trends & Issues in Crime and Criminal Justice, 374,* 1-6.

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management, 8*(3), 238-264.

Ries, E. (2011). *The Lean Startup*. New York: Crown Business.

Robbins, S. P., & Judge, T. A. (2012). *Essentials of Organizational Behaviour* (11th ed.). Essex: Pearson Education Limited.

Roth, P. A. (1987). *Meaning And Method In The Social Sciences A Case For Methodological Pluralism*. London: Cornell University Press.

Rowbottom, R., & Billis, D. (1977). The stratification of work and organizational design. *Human Relations, 30*(1), 53-76.

Sadler-Smith, E., & Shefy, E. (2004). The intuitive executive: Understanding and applying 'gut feel' in decision-making. *Academy of Management Executive, 18*(4), 76-91.

Saldana, J. (2009). *The Coding Manual for Qualitaive Researchers*. London: SAGE Publications.

Sammarra, A., Profili, S., & Innocenti, L. (2012). Do external careers pay off for both managers and professionals? The effect of inter-organizational mobility on objective career success. *The International Journal of Human Resource Management, 24*(13), 2490-2511.

Sarre, R., & Prenzler, T. (2000). The relationship between police and private security: Models and future directions. *International Journal of Comparative and Applied Criminal Justice, 24*(1), 91-113. doi:10.1080/01924036.2000.9678654

Scott, R. W., & Gerald, D., F. (2007). *Organizations and Organizing: Rational, Natural and Open Systems Perspectives*. New York: Routledge.

Selander, S. (1990). *Associative strategies in the process of professionalization: professional srategies and scientifcation of occupations* (M. Burrage & R. Torstendahl Eds.). London: SAGE Publications Ltd.

Sennewald, C. A. (2011). *Effective Security Management* (5th ed.). Portland: Butterworth-Heinemann.

Simonsen, C. (1996). The case for: security management is a profession. *International Journal Of Risk, Security And Crime Prevention, 1*(3), 229-232.

Sims, C., A. (1996). Macroeconomics and methodology. *Journal of Economic Perspectives, 10*(1), 105-120.

Slovic, P., Peters, E., Finucane, M., & MacGregor, D. G. (2005). Affect, risk, and decision making. *Health Psychology, 24*(4S), 1-30.

Smith, A. (1775/2007). *An Inquiry into the Nature and Causes of the Wealth of Nations* S. M. Soares (Ed.) Retrieved from https://www.ibiblio.org/ml/libri/s/SmithA_WealthNations_p.pdf

Smith, C., & Robinson, M. (1999). *The understanding of security technology and its applications.* Paper presented at the 1999 International Carnahan Conference on Security Technology.

Somerson, I. S. (2009). *The Art And Science Of Security Risk Assessment*. Alexandria: ASIS International.

Speer, J., D.,. (2017). Pre-market skills, occupational choice, and career progression. *Journal of Human Resources, 52*(1), 187-246.

Stamp, G. (1981). Levels and types of managerial capability. *Journal of Management Studies, 18*(3), 277-298.

Steden, R. V., & Sarre, R. (2007). The growth of privatized policing: some cross-national data and comparisons. *International Journal of Comparative and Applied Criminal Justice, 31*(1), 51-71.

Stewart, D. W., Shamdasani, P. N., & Rook, D. W. (2007). *Focus Groups* (2nd ed.). Thousand Oaks, CA: SAGE Publications Inc.

Stichweh, R. (2008). The eigenstructures of world society and the regional cultures of the world. In I. Rossi (Ed.), *Frontiers of Globalization Research* (pp. 133-151). New York: Springer.

Strauss, A. L. (1975/2001). *Professions, Work and Careers*. New Jersey: Transaction, Inc.

Sutton, J., & Austin, Z. (2015). Qualitative research: data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy, 68*(3), 226-231.

Talbot, J., & Jakeman, M. (2009). *Security Risk Management Body of Knowledge*. New Jersey: Wiley.

Thacher, D. (2006). The normative case study. *American Journal of Sociology, 111*(6), 1631-1676.

Torstendahl, R. (1990). Promotion and strategies of knowledge-based groups. In R. Torstendahl & M. Burrage (Eds.), *The Formation of Professions* (pp. 1-10). London: SAGE Publications Inc.

Wakefield, A. (2014). Where next for the professionalization of security? In Gill (Ed.), *The Handbook of Security* (pp. 919-935). London: Palgrave Macmillan UK.

Walby, K., & Lippert, R. (2014). *Corporate Security In The 21st Century : Theory And Practice In International Perspective.* Basingstoke: Palgrave Macmillian.

Walby, K., Wilkinson, B., & Lippert, R. K. (2014). Legitimacy, professionalisation and expertise in public sector Corporate Security. *Policing and Society*. *26*(1), 38-54.

Weber, M. (1947). *The Theory of Social and Economic Organization* A. M. Henderson (Ed.) Retrieved from http://solomon.sth2.alexanderstreet.com.ezproxy.ecu.edu.au/cgi-bin/asp/philo/sth2/documentidx.pl?sourceid=S10020412

Webster, E. (2001). The rise of intangible capital and labour market segmentation. *Australian Bulletin of Labour, 27*(4), 258-271.

Weeden, K., A.,. (2002). Why do some occupations pay more than others? Social closure and earnings inequality in the united states. *American Journal of Sociology, 1*(108), 55-101.

White, J. (2014). *Security Risk Assessment Managing Physical and Operational Security. Burlington*: Elsevier Science.

Wilensky, H. L. (1964). The professionalization of everyone? *American Journal of Sociology, 70*(2), 137-158.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis, 27*(3), 597-606.

Witte, R. S., & Witte, J. S. (2017). *Statistics* (11th ed.). New Jersey: John Wiley & Sons, Inc.

Worren, N. A., Moore, K., & Elliott, R. (2002). When theories become tools: Toward a framework for pragmatic validity. *Human Relations, 55*(10), 1227-1250.

Wrzesniewski, A., McCauley, C., Rozin, P., & Schwartz, B. (1997). Jobs, careers, and callings: people's relations to their work. *Journal of Research in Personality, 31*(1), 21-33.

Yin, R. K. (2014). *Case Study Research: Design And Methods* (5th ed.). Los Angeles: SAGE.

APPENDIX A PHASE ONE SURVEY QUESTIONNAIRE

1. What is your Job Title?
2. Which of the following Job titles would you say is closest to your functional equal?

Chief Executive Officer | Executive Vice President | Vice President | General Manager | Unit Manager | Front Line Manager | Front Line Worker

3. How many employees do you manage?

[continued over page]

When answering these questions, please consider the ***longest*** time you have taken in your current position, not the average or most common times.

Work Measurement Scale	1 Day – 3 Months	3 Months – 1 Year	1 Year – 2 Years	2 Years – 5 Years	5 Years – 10 Years	10 Years – 20 Years	20+ Years	Not Applicable
In what time frame do you plan for the future?								
In what time frame do you allocate resources into the future?								
How far into the future is your longest work assignment?								
What is the longest time frame you expect a subordinate to complete work assignments?								
In what time frame do you expect financial return on investments?								
How far into the future are you planning the development of staff? (Training, Experience)								
How far into the future are you identifying threats in your risk management process?								
What is the longest implementation time for risk mitigation strategies?								
What is the longest period of time a superior has given you to complete a task?								
How long does it take you to complete your most common longest task?								

When answering these questions, please consider ***your own, personal work*** and how strongly you agree or disagree with each statement

Task Complexity Measurement Tool	Very Strongly Disagree	Strongly Disagree	Disagree	Agree	Strongly Agree	Very Strongly Agree
4. My work is done by following an assigned plan to a goal, over-coming obstacles by direct actions and trial-and-error	1	2	3	4	5	6
5. My work involves collecting information about a defined problem and using that information to develop a solution or make a decision.	1	2	3	4	5	6
6. My work requires planning for future needs in consideration of current needs, as well as develops alternative plans as a backup.	1	2	3	4	5	6
7. My work requires the management of a number of projects which must be adjusted and undertaken in relation to each other	1	2	3	4	5	6
8. My work requires an understanding of the immediate and downstream consequences on my organisation if any aspect of a project is changed.	1	2	3	4	5	6
9. My work requires me to remain up to date and knowledgeable about the business environment, favourably influencing any and all developments which may have significance to current projects being undertaken	1	2	3	4	5	6
10. My work requires the development of world-wide strategic options and the creation of business units, by growth, acquisition, mergers and joint ventures	1	2	3	4	5	6

APPENDIX B PHASE TWO INTERVIEW GUIDE

No.		Question
1	Occupational Success	Could you explain how you started work in the security industry?
2		Could you explain your work experience?
3		Can you talk about the duties you undertake in your role?
4		Could you elaborate on the value security brings to your organisation?
5	Organisation Complexity	How complicated is your work?
6		Could you explain the unique stresses that come with a security role?
7		When you make decisions and start a task or project, is there a lot of uncertainty that you have to deal with?
8		Is the security environment changing faster now than it has been in the past?
9	Progression Ceiling	Could you explain what career pathways are open to you with your security experience?
10		How would you 'move up' in the organisation with a security background?
11		Do you think there is a point where security managers need to leave security to progress into more senior roles in an organisation?

APPENDIX C ETHICS AND CONSENT FORMS

Phase One Survey Consent Cover

Dear Participant,

My name is Codee Ludbey and I am a Masters by Research student in the School of Science at Edith Cowan University. You are invited to participate in a research project which is being conducted as part of my thesis.

The purpose of this project is to investigate the Corporate Security industries structure within organisations, and the perceived glass ceiling in the profession.

Participants in this research must be at least 18 years of age, and be actively working within the security industry. Should you choose to participate in this project, you will be asked to complete a short online survey with a series of questions related to the general nature of your work. there are no 'correct' answers, I am only seeking your honest opinion about this topic. The survey should take approximately 5 minutes.

The online survey will be anonymous with no personal information collected outside of your Job title. Only the project supervisor and I will have access to the answers that you provide, and we will not be capable of identifying you with these answers.

Access to the collected data will be limited and stored securely. Participation in this project is voluntary and you are free to withdraw at any time until the completion of the survey at which point it becomes impossible to identify you.

If you have any questions or require any further information about the research project, please feel free to contact either myself or my supervisor Dr. Dave Brooks.

By clicking the below link to proceed, you are providing consent to participate in this research, accepting that your responses will be anonymous.

Thank you,

Codee Roy Ludbey
BSc (Security)
cludbey@our.ecu.edu.au
[redacted]

Other Contacts

Dr. Dave Brooks
Edith Cowan University
100 Joondalup Drive, JOONDALUP WA 6027
d.brooks@ecu.edu.au
Phone: +61 8 6304 5788

HUMAN RESEARCH ETHICS COMMITTEE
Research Ethics Officer
Edith Cowan University
270 Joondalup Drive, JOONDALUP WA 6027
Email: research.ethics@ecu.edu.au
Phone: +61 8 6304 2170, Fax: 6304 2661

Phase Two Handout

Dear Participant,

My name is Codee Ludbey and I am a Masters by Research student in the School of Science at Edith Cowan University. You are invited to participate in a research project which is being conducted as part of my thesis.

The purpose of this project is to investigate the Corporate Security industries structure within organisations, and the perceived glass ceiling in the profession.

Participants in this research must be at least 18 years of age, and be actively working within the security industry. Should you choose to participate in this project, you will be asked to take part in a focus group with your peers. The focus group interview will take place in a central office within the CBD ([redacted]). There will be a discussion related to the general nature of your work. there are no 'correct' answers, I am only seeking your honest opinion about this topic. The focus group will take approximately one hour.

Importantly, if you are to take part in this research, you will need to keep information learned about other participants confidential.

Attached to this form is a Consent Form which you are required to fill out, and a list of Career Counselling Services should you wish to consult a professional after taking part in this research.

Confidentiality

Confidentiality will be of upmost importance from start to finish of this project. All information provided by you will be treated with respect and all identifying information will be removed. The information you provide will allow me to draw comparisons between participants and identify key understandings of security. The raw information provided by you will only be seen by myself and my supervisor.

All focus group interviews will be recorded, however once this information has been transcribed - and your name replaced with a pseudonym (e.g. Participant 1), the original recording will be erased. The data recorded will be stored on a digital tape recorder for a period of up to one (1) month before deletion.

Access to the collected data will be limited and stored securely. Participation in this project is voluntary and you are free to withdraw at any time until the data collected has been anonymised, at which point it becomes impossible to identify you.

If you have any about the research project, please feel free to contact those listed below.

Thank you,

Codee Roy Ludbey

cludbey@our.ecu.edu.au

Other Contacts

Dr. Dave Brooks

Edith Cowan University

100 Joondalup Drive, JOONDALUP WA 6027

d.brooks@ecu.edu.au

Phone: +61 8 6304 5788

HUMAN RESEARCH ETHICS COMMITTEE

Research Ethics Officer

Edith Cowan University

270 Joondalup Drive, JOONDALUP WA 6027

Email: research.ethics@ecu.edu.au

Phone: +61 8 6304 2170, Fax: 6304 2661

Consent Form

By signing this consent form you are agreeing to participate in the research outlined in the 'Information Letter to Participants' letter. You also confirm that you have been provided with said letter, and understand all information provided. You agree that you have been given the opportunity to ask questions and had any questions asked answered to your satisfaction. You understand that you can ask further questions at any time. You are aware that you can withdraw from the research project at any time prior to your information being anonymized, at which point you cannot be identified.

You also understand that you will be required to undertake a one hour focus group session which will be recorded, and are comfortable with the measures outlined in the information letter as to how this information will be handled, stored, and destroyed. You also understand that this information will only be used for the purposes of this research project.

You also understand that you are free of any and all obligations towards this research, and have agreed to undertake this research of your own free will.

I, Name:_____, agree with the above and give my consent to participate in this research project as of Date:_____.

Signature:_____

APPENDIX D PHASE ONE SURVEY RESPONSE DATA

Organisation	Job Title	Assignment	Time to Complete	Employees	Job Level	WMS	TCMT	Average
One	Director of Security	Develop, deliver strategy	Incomplete	8	6	4	6	5
One	National Risk and Security Manager	Overseeing operational risk and security within organisation	Ongoing	3	3	3	7	4
One	Senior intelligence analyst	Threat analysis	1-2 days	0	1	2	6	3
One	Senior risk and security manager	Create a safety environment and culture while making sure I have a good coordinated emergency response team.	Ongoing task which can take 1-2 hours every day	28	3	2	7	4
One	National Risk and Security Operations Manager	Project management	60% of work time	2	3	2	7	4
One	Risk and Security Manager 1	Training / Consultation	Approx 20 hours per work	14	2	3	6	4
One	Risk and Security Manager 2	Dealing with public liability incidents	1 hour a day	12	2	2	4	3
One	Risk and Security Manager 3	Responding to requests	1 hour	7	3	3	6	4
One	Risk and Security Supervisor	First Aid	15-30 minutes	13	3	1	6	3
One	Risk and Security Manager 4	Asset and Brand Protection	2 hours	20	3	2	6	4

Organisation	Job Title	Assignment	Time to Complete	Employees	Job Level	WMS	TCMT	Average
One	Manager, Global Intelligence and Threat Analysis	Threat analysis	Ongoing	2	3	2	7	4
One	Security Supervisor	Customer Relations	15 min	25	2	2	6	3
One	Security Supervisor	Signing off on reports	2 hours	27	1	1	6	3
One	Technical manager	Incomplete	Incomplete	2	3	3	7	4
One	Regional Manager Risk and Security	Coordination of the risk and security function in the organisation	All day	6	3	2	6	4
One	Senior Risk and Security Manager	Managing the risk and security for the organisation in a specific location	Ongoing	9	2	3	7	4
One	Risk Security Manager 5	Manage security and life safety incidents	It depends on the incident	12	2	2	7	4
One	Senior Risk and Security Manager	Security and Public liability related matters	3.5 days out of 5 working days	17	2	3	7	4
One	Risk and Security Manager	People management	Changes every day	10	3	2	7	4
Two	Executive Manager Group Security	Oversee security functionality	Incomplete	160	5	3	7	5
Two	Senior manager, Corporate Security design and assurance	Manage projects	Various	2	3	2	4	3

Organisation	Job Title	Assignment	Time to Complete	Employees	Job Level	WMS	TCMT	Average
Two	Security operations manager	Day to day security operations management	Incomplete	3	3	3	5	4
Two	Security systems administrator	Security install projects	3 months	5	2	2	6	3
Two	Incomplete	Collation of physical and operational risk assessments	2 hours	1	2	3	6	4
Three	National Security director	Representation and policy	Incomplete	90	6	4	7	6
Three	Facilities/security manager	Reports and meetings	3 hours per day	500	2	2	7	4
Three	Regional Security Manager	Security compliance and process	50% of my time	0	2	2	4	3
Three	Senior intelligence analyst	Daily reporting to clients	2 hours	0	1	1	7	3
Three	Intelligence analyst	Reports	1 week	0	1	1	1	1
Three	Security officer	Personnel security	3 hours a day	6	2	4	6	4
Four	Director of Surveillance	Staff Management	2 hours / day	6	3	1	5	3
Four	Protection Manager	Analyse data	4 hours	3	2	2	7	4
Four	Surveillance Training Coordinator	Training Staff	4 Weeks	4	2	1	6	3
Four	Surveillance Operator	Monitor CCTV	10 hours	3	1	1	6	3

Organisation	Job Title	Assignment	Time to Complete	Employees	Job Level	WMS	TCMT	Average
Four	Surveillance Supervisor	Ensure integrity of organisation	6 hours	3	2	1	2	2
Four	Director of Security	Managing Change	1 hour	150	3	3	7	4
Four	Risk & Compliance Manager	Risk Management	14 days	34	3	2	6	4
Four	Surveillance Supervisor	Evaluate potential threats	1 hour	3	3	1	6	3
Four	Operations Manager	Managing incidents	1 hour	120	3	1	6	3

APPENDIX E TRANSCRIPTS WITH MANUAL CODING

This appendix has been restricted from Research Online.

APPENDIX F CODING TABLE

This appendix has been restricted from Research Online.