Edith Cowan University

Research Online

Theses : Honours

Theses

2016

The corporate security stratum of work: Identifying levels of work in the domain

Codee Roy Ludbey
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

 Part of the Business Commons, and the Information Security Commons

Recommended Citation

Ludbey, C. R. (2016). *The corporate security stratum of work: Identifying levels of work in the domain.* https://ro.ecu.edu.au/theses_hons/1489

This Thesis is posted at Research Online.
https://ro.ecu.edu.au/theses_hons/1489

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author's moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

The corporate security stratum of work: Identifying levels of work in the domain

This thesis is presented in partial fulfilment of the degree
of
Bachelor of Science (Security) Honours

Codee Roy Ludbey

Edith Cowan University

School of Science

2016

ABSTRACT

Corporate security is a practicing domain and developing academic discipline that provides for the protection of people, information and assets, as well as the self-protection of organisations. Fayol (1949) articulated such an activity within organisations to be a core business function of significant importance; embedding security operations within all aspects of organisational work. This embedded nature of security within organisations has led to difficulty in the literature delineating roles and responsibilities of security practitioners; consequently leading to a nebulous understanding of security as a whole. Therefore, an investigation of the corporate security stratum of work has been undertaken to address this issue in part, undertaking an innovative, objective approach. The study embraced the broader socio-organisational literature to ground and orient the research, providing an outward-in perspective in its exploration of the corporate security function.

The research perspective was rooted in the sociological theory of structural functionalism, where Parsons (1951) and Durkheim (1984) identified an occupational stratum of work seated within a differentiated and stratified society. Such a society induces individuals to fulfil specialist roles, which can be ranked hierarchically along a stratum of work. Significantly, organisations are the practical implementation of this occupational stratum of work, with specialist roles aligned hierarchically and controlled through positions of authority. Jaques (1951, 2002) articulated seven strata of work within organisations, each delineated by their capacity to understand complexity and capability to manage tasks into the future.

This study undertook an ethnographic approach, consisting of two parts. Firstly, the literature critique informed the design and implementation of the research instrument; which consisted of two tools. Secondly, the administration of the research instrument to the participant sample, which was refined through a pilot study (N=16) and then applied to the main study (N=42). The study identified a suitable sample consisting of security practitioners functionally positioned across the stratum of work, with this sample being purposively selected.

Significantly, the study revealed a disconnect between the corporate security and socio-organisational literature, with many points of divergence. Such disconnect is rooted in a misperception of the importance and positioning of the corporate security function by the corporate security literature. Therefore, the study has revealed that corporate security operates at a tactical and operational level within an organisation, functionally positioned between Stratum One and Stratum Four. This finding indicates that the concept of corporate security as a strategic function with executive reach is invalid, and the existence of a strategic security practitioner is not the norm. Furthermore, the study has established the corporate security function as an operating activity situated within the technostructure of organisations; leveraging its ability to diagnose, infer, and treat discipline specific concerns.

Subsequently, these findings have uncovered several significant implications for policy, education, academia, and the broader community. These implications include career progression pathways and an understanding of the glass ceiling for security practitioners; professionalisation of the industry, including insights into corporate perceptions of the function; corporate security practitioner role definition and articulation, where defined jurisdictional boundaries can be begin to be drawn; and the fallout of a misaligned corporate security literature consensus.

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: 3/11/2015

ACKNOWLEDGEMENTS

I would like to sincerely thank and acknowledge my supervisors; Dr. David Brooks and Dr. Michael Coole for their continuous support, advice, guidance, and patience throughout both my undergraduate study and this thesis - thank you.

I would also like to thank my friends and family for their continued patience and support in this, and every other endeavour - thank you.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

Published

Ludbey, C. (2015). The stratum of work in the security industry: Perceptions of the application of security in the corporate organisation. *Australian Security Magazine, JUNE/JULY,* 24-25.

Abstract: Corporate security is continuing through a period of growing pains, with corporate executives and security managers often failing to agree on the value of the function. This disparity must be addressed, not through overselling threats and fear-mongering, but through addressing fundamental concerns of organisational structure and responsibility.

Under Peer Review

Ludbey, C., & Brooks, D. (n.d.). Stratum of Security Practice: Using Risk as a Point of Measure in the Stratification of Security Works. *Security Journal*

Abstract: Corporate security is a unique practice area within the broad security domain, providing security across government and private organisations. Nevertheless, an understanding of the hierarchy and influence of corporate security practitioners within an organisation is lacking. In contrast, security literature claims that senior security practitioners occupy the executive levels of organisational management. Therefore, the study investigated the link between the measure of risk uncertainty and the level of work in a role, using Jaques' general theory of managerial hierarchies.

The study findings demonstrated that within corporate security, risk does provide a measure of work stratification that indicates a relationship between risk scanning and work level. Furthermore, that this identified the hierarchy of security within the broader corporate stratification of work. Results indicate that the higher the person is within the work strata, the broader and more external their scanning of risk. However, the security manager may hold a senior executive title but lacks alignment in risk outlook and level of work when compared to other executive managers.

Ludbey, C., Brooks, D., & Coole, M. (n.d.). Corporate Security: Identifying and Understanding Levels of Work in the Domain. *Security Journal*

Abstract: The corporate security activity area within organisations was first identified by Fayol (1949) as functionally significant. Nevertheless, corporate security remains ill-defined, unstructured, and not well understood. Thus, the study undertook an examination of the corporate security function through the lens of the broader socio-organisational literature to uncover corporate security's seating and focus as an organisational function. The study's findings indicate that the corporate security function operates at the operational and tactical strata of an organisation, with no strategic impact. Furthermore, findings support the positioning of the corporate security function within organisations is within the technostructure, which is responsible for providing analytical support to business operations. Consequently, the study identified a significant disconnect between the corporate security literature, as written by security practitioners and academia, and the socio-organisational literature, with many identified points of divergence. Evidence of this divergence was revealed through identification of work levels within the corporate security function.

CHAPTER ONE: INTRODUCTION

Security and in particular, corporate security, is a developing academic discipline that is immersed in the management of risk (Smith & Brooks, 2012, pp. 51-79). Significantly, the discipline is a practicing domain that provides for the protection of people, information and assets within an organisation; with its objectives to provide for the self-protection of a corporation. Brooks and Corkill (2014) contend that corporate security's activities enable the executive team to exercise control and governance across the organisation in the face of malevolent threats. Consequently, as a practising domain corporate security undertakes a broad range of activities across multiple domain agent groups. However, corporate security remains an under researched area of practice, with poorly defined and articulated boundaries and structure resulting in an immature and ill-defined occupational stream. Such a dearth of understanding means that corporate security objectives may not be completely achieved, negatively impacting on broader corporate objectives, and that the career prospects for its practitioners are hindered as they attempt to climb the corporate ladder.

If corporate security is to advance in its maturity, then it requires better understanding of its undefined boundaries and structure. It is argued that the nature of an effective corporate security function requires access transversely and hierarchically across an organisation (Sennewald, 2011). For this to be achieved clarity is required in relation to corporate security's seating within an organisation, its hierarchical structure, sphere of influence, and barriers to executive access. Therefore, the ability to accurately measure, define, and understand the corporate security function is significantly important if the practicing domain is to grow in its maturity, scope, and sphere of influence. In part, this study begins to address some of these issues.

1.1 Background of the Study

Corporate security is an organisational undertaking with the function to provide services which ensure stability and protection of business operations from malicious disruption and harm (Talbot & Jakeman, 2009). Furthermore, the application of corporate security is underpinned by the implementation of policy and functionally achieved through a combination of procedural, technical and physical risk strategies and control measures (Smith & Brooks, 2012). Consequently, corporate security transforms organisational resources through the application of management practices into a protective business function. Such security activities were argued by Fayol (1949) to represent an essential business function for every organisation.

The necessity of these security activities within an organisation place security practitioners within the organisations management team and associated corporate strata. However, it has been argued that corporate security managers are under-represented within the higher management strata of organisations irrespective of their essential function in facilitating the achievement of organisational objectives (McGee, 2006; Cubbage & Brooks, 2013; Brooks & Corkill, 2014). Accordingly, this study sought to investigate the contemporary stratification of work within the corporate security management domain to understand how this stratum aligns with the broader corporate management strata.

The practice of corporate security has often been considered from a managerial context. As a result of this, effective security managers view their outputs as contributors to overall business objectives (Smith & Brooks, 2012); seeking to align their function to the whole organisation (Sennewald, 2011). Such a position can be historically traced to early theorists of scientific management, where Fayol (1949) purported security to be, among others, a core business activity of every organisation. Historically, organisational management fitted within the broader corporate business strata, for instance, Jaques (1996) highlighted seven levels of occupational strata aligned to key business task indicators, through coupling a roles' task complexity with its time-span of discretion. Such coupling enabled the articulation of organisational role seating within the broader organisational span of control chart.

In contemporary times corporations have expanded, with many becoming global business operations embodying both rewards and risks (Rossi, 2008; Robbins & Judge, 2010). Consequently, the global business environment has seen the strata of management within organisations undergo significant changes (Rossi, 2008). Such changes include for example, the transforming structure of organisation's executive level strata (Stichweh, 2008), reduction in temporal-spatial restrictions which have influenced organisational design (Rossi, 2008), and the introduction of automation and outsourcing.

Subsequently, it is argued that security management has not been raised in the contemporary business environment to the executive level. Nevertheless, many security practitioners believe that security should be operated within the executive stratum of work (Sennewald, 2011; Cubbage & Brooks, 2013). Such a position is believed to aid effective decision making and long term alignment between security operations and business objectives in the management of security risk. Nevertheless, such a view appears not to be accepted by the corporate world. McGee (2006) suggests that security is perceived as a lower strata function with no strategic weight within many organisations. Consequently, this disparity in views must be addressed through an understanding of the actual role and function achieved by the corporate security occupations within the organisational context.

1.1 Purpose Statement

The study investigated the stratum of work in the corporate security function within organisations. This investigation was directed to understand the disparity of views inherent in the literature, addressing the positioning and reach of the corporate security function. Consequently, the study focused on uncovering the extent to which the corporate security stratum of work permeates hierarchically within organisations. To approach this investigation, the study was underpinned by the sociological theory of structural functionalism, which purports an occupational stratum of work is inherently specialised in the provision of roles to society. Consequently, this theory provided leverage for the study to tabulate the levels of work within the corporate security function through alignment to the broader socio-organisational literature. Further, through leveraging this alignment, the study could uncover the functional positioning of corporate security within organisations.

1.2 Study Objectives

The objectives of the study were to;

1. Understand the alignment of corporate security to the broader socio-organisational literature;
2. Uncover the stratum of work in the corporate security function;
3. Discover the extent to which corporate security permeates organisations;
4. Identify the functional positioning of the corporate security function within organisations.

1.3 Research Questions

The study explored the stratum of work in the corporate security function within organisations. The study responded to two questions arising from a perceived gap in the corporate security literature:

(1) What is the stratum of security practitioners in the corporate organisation context?

The study investigated the stratum of work in the corporate organisation context through the lens of the broader socio-organisational literature. Through examination of the corporate security business function from this context, it was reasoned that the positioning of corporate security work could be uncovered within the broader occupational stratum of work.

(2) To what extent does the corporate security function permeate throughout organisations?

The study sought to understand the alignment of the corporate security practice area with the broader socio-organisational literature to reveal the positioning of the corporate security function within organisations. The exploration of this positioning provides significance in the broader literature discussion about professionalisation in the industry and the jurisdictional boundaries of work for the corporate security function.

1.4 Significance

A significant disparity exists in the security literature regarding the positioning, functional influence of the corporate security practice area, and professional advancement for corporate security managers. Such a disparity has several implications for education, industry, and academia. Consequently, the study is significant as it undertook an innovative and objective approach to fundamentally understand this issue within the context of the stratum of work in the corporate security domain. To achieve this, the study aligned the corporate security function to the broader socio-organisational literature, extricating itself from any inherent bias or potential misconceptions in the corporate security literature. Axiomatically, this fundamentally shifts the research approach, ensuring corporate security is considered from the broader context of corporate organisations.

Furthermore, by adopting this broad and external viewpoint to the function, the study identified the stratum of work inherent in the corporate security domain, and uncovered its functional seating within organisations. Such revelations significantly shift the way in which corporate security is perceived, shaping education standards, academic discourse, and impacting regulatory and legislative controls on the practicing domain. Additionally, this fundamental shift in understanding

clearly articulates why practitioners struggle to break through the corporate glass ceiling and reach the executive strata of work. Thus, such a fundamental shift provides a starting point for the genesis of new perspectives and understandings of the corporate security function within organisations.

1.5 Overview of the Study

The thesis is comprised of seven chapters including this introduction. The following chapters are summarised:

Chapter Two: Underlying Theory and Review of the Literature

Chapter Two provides the orientation and grounding of the study through the presentation of models and frameworks. The underlying theory of structural functionalism provided a starting point for the research and highlighted key elements for consideration in the literature review. From this starting point, the literature review explored the key areas of research; namely, the broader socio-organisational literature and the corporate security literature. An exploration of these bodies of work highlighted numerous gaps and provided justification and a framework for the methodology.

Chapter Three: Methodology

The methodology chapter outlined the procedures and methods used in the collection of data for both the pilot study and the main study. This outline includes sampling considerations, alongside the justification for the creation of a research instrument with a new measurement tool. The discussion explores the process through which this instrument was graded, and identifies potential limitations. Finally, the reliability and validity of the methodology is discussed, providing context for the data analysis in the following chapters.

Chapter Four: Pilot Study

Chapter Four articulates the process, analysis and findings of the pilot study. The pilot study tested the methodology against a small sample, providing insight into the research instrument's construction. Furthermore, through the analysis of the collected data testing of the methodological approach was achieved, flagging potential shortfalls or further limitations not considered in the methodology chapter. Considering this analysis, the chapter continues to outline the findings and their implications for the main study, setting the stage for interpretation and discussion. The chapter concludes by suggesting some minor changes to the research instrument for use in the main study, honing the data collection methodology in the process.

Chapter Five: Analysis

Chapter Five presents the study's data analysis, specifically tabulating the survey responses and classifying them into their identified stratum of work. Through this classification, the chapter explored the identified work level of each respondent, alongside their job title and number of employees managed. This data was then further analysed, reflected on, and discussed, with the inclusion of a calculated mean level of work and standard deviation between measurement tools. Within Chapter Five, the research instruments reliability and validity is also discussed, with each tool in the instrument investigated in relation to the data collected.

Chapter Six: Interpretation and Discussion

Chapter Six reflects further on the analysis findings and provides an interpretation and discussion in response to the study's postulated research questions. The interpretations of the study's findings are discussed in conjunction with the literature, with significant findings being outlined and considered.

Chapter Seven: Conclusion and Findings

The final chapter provided a summation of the work conducted throughout the thesis, and synthesised the significant findings of the study in response to the research questions. The chapter continues by outlining the potential theoretical and policy implications for these findings. The chapter concludes with the provision of some recommendations, and an outline of the limitations of the study.

1.6 Conclusion

This chapter presented the background of the study, identifying the core drivers for the research, and illuminating key issues for exploration. Consequently, consideration of the corporate security stratum of work has been identified as a significant and relevant topic of interest to the corporate security literature, requiring an innovative and more objective approach to be undertaken. This study therefore explored this stratum of work, alongside its permeation throughout modern organisations by adopting the perspective of the broader socio-organisational literature. Accordingly, this perspective provided a holistic and unique approach through which observations of the corporate security function could occur. Evidence for the significance of this approach will be elaborated in the following chapter, where the insular and isolated corporate security literature is critically examined; and a case for its alignment to the broader socio-organisational literature is argued.

CHAPTER TWO: UNDERLYING THEORY AND THE LITERATURE INFORMING THIS STUDY

This chapter presents the underlying theory of structural functionalism and the socio-organisational literature supporting the study. The chapter details the interrelationship between these bodies of work to explore the concept of an occupational stratum of work in society, and its natural application through organisations. This natural application of the occupational stratum of work is examined through Jaques (1996), who provides a framework through which work can be divided, specialised, and considered. Through embedding a sociological perspective to this study, the review of the corporate security literature was conducted from an external point of view. This approach provides an opportunity to capture the corporate security function from an objective viewpoint, aligning it to the broader socio-organisational literature.

2.1 Sociological Theory of Structural Functionalism

The theory of structural functionalism is grounded in the observation that society is a system. This system is embedded within the concept of a social cultural consensus with various parts that can be differentiated and stratified. Nevertheless, these parts are all interdependent and together form more than their sum. Durkheim's (1984, p. 79) work posited the natural systemic state of a society is one of social and cultural consensus. Furthermore, Durkheim developed the idea that within a model of social consensus, there is differentiation; and over time, societies change, adapt, and evolve to become more specialised reinforcing this model of differentiation (Durkheim, 1984; Roberts, 2012, p. 55).

Considering this, society is then made up of more than just individuals; it includes systemic aspects of a society. These aspects include the economic system, the fiduciary system, and the political system (Durkheim, 1984, p. 154; O'Byrne, 2013, p. 30). Such societal systems are divided according to specialisations, which are again further sub-divided into particular roles and outputs (Davis & Moore, 1945; Dillon, 2013, p. 94; Wilensky, 1964). This division of societal systems was discussed by Parsons (1951); postulating that society is divisible into four primary sub-systems required to survive, namely; adaptation (economic), goal attainment (political), system integration (legal), and pattern maintenance or latency (cultural). These sub-systems encompass the actions of all individuals, and the conduct of any action or change in one sub-system directly impacts another (Dillon, 2013, p. 159; O'Byrne, 2013, p. 29). Furthermore, the roles of these sub-systems can be competitive and this can cause strain on society. Individual action through any of these sub-systems can enact societal change depending on their role.

Parsons (1951, p. 26) examined the role of individuals and things within these societal sub-systems, drawing from work established by Davis and Moore (1945). It was considered that the distribution of members in a society can be attributed to the inducement of individuals into required roles by means of motivation and desire. Such inducements come through access to sustenance and comfort, humour and diversion, and self-respect and ego (Davis & Moore, 1945). Parsons (1951) aligned this concept of inducements to societal status, arguing that an individual's location or status in the societal system is related to their functional significance.

Dillon (2013, p. 173) deliberates that stratified positions within society are hierarchically ranked through their importance to the societal system, and the complexity or training and talent required to fulfil the role. All positions within society require some level of skill and capacity to perform the duties of the role, and this is achieved either through natural capacity or training and education (Davis & Moore, 1945). Finally, it is posited that the more culturally complex a society, the higher the level of specialisation (Davis & Moore, 1945). The influential work of Wilensky (1964) discussed this in terms of proffesionalisation, where there is a push from many occupations to be considered 'professionals', with a seating towards the top of the occupational stratum.

2.1.1 Criticisms of Structural Functionalism

Structural functionalism as a theory of society is not without its criticisms. Two systemic criticisms of structural functionalism are that it cannot deal with change, and it cannot deal with dysfunction (O'Byrne, 2013, p. 27). In light of these criticisms, Chilcott (1998) posits the idea that functionalism can still be useful in understanding and explaining a phenomenon or culture. Chilcott argues that structural functionalism, as an articulation of society, can be used to develop theories and explanations within ethnographic approaches to research. Davis (1959) had a similar view, stating that functionalist approaches are simply generic sociological approaches which can be useful in the conduct of research.

This study draws on structural functionalism as a sociological grounding, as the notion of a stratified occupational society divided according to task specialisation is congruent with the influential work of Fayol, Jaques, and Mintzberg informing this study.

2.2 Organisations and Management

The hierarchical ranking of positions and roles in society through the specialisation of work, and the functional significance of such work leads to the idea of an occupational stratum of work (Dillon, 2013). This occupational stratum of work is embedded in all aspects of society, and is most readily seen in organisations. As Litterer defines it, organisations are "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).

This articulation is supported by Mahajan (2010), Martin and Fellenz (2010), and Robbins and Judge, (2012) who explain that organisations are a vehicle for accomplishing goals and objectives through a system of interpersonal relationships aligned to a structure of authority, status and role. It is argued that this structure of authority, status, and role is directly related to, and is the natural application of, the occupational stratum of work (Parsons, 1951; Dillon, 2013).

Organisations are created through a process that involves the identification of the goals of the organisation, and the activities required to achieve these goals (Mahajan, 2010). Once created, the division of said activities into specialised roles must be undertaken to outline the processes and sub-processes required to achieve these derived goals (Martin & Fellenz, 2010). The grouping of roles according to a hierarchy is considered, allowing for structure to form (Mahajan, 2010). Once the underlying structure of the organisation is outlined, the chain of responsibility, command, and authority is delegated appropriately, and the processes of achieving the organisations goals are set into motion (Mahajan, 2010).

It is considered that organisations are linked to the environment around them, and have the ability to produce their own context and culture to deal with this environment. The ideal outcome of an organisation is to reduce ambiguity and uncertainty in achieving set goals and objectives (Mahajan, 2010).

It is important to understand that all organisations consist of the following elements;

- Activities: The processes and tasks assigned and completed to achieve an organisational goal or objective;
- Authority: The delegation of tasks in aid of more efficient achievement of goals;
- Coordination: Working relationships whereby decisions and actions are harmonised across the organisation in aid of achieving activities, goals, and objectives;
- Environment: The external environment within which the organisation operates; and
- Objectives and plans: The element of the organisation that provides direction and unification of work (Jaques, 1996; Litterer, 1963; Mahajan, 2010; Martin & Fellenz, 2010; Mintzberg, 1980; Robbins & Judge, 2012).

Such organisational elements provide a framework through which other management functions can be performed in pursuit of greater goals and objectives. Management is considered a sub-process of organisations that involves planning, organising, leading and controlling of resources (Martin & Fellenz, 2010). The outcome of effective management is the reduction of ambiguity in goal setting, the facilitation of coordination between roles, departments, and activities, and employee development and efficiency (Jaques, 1996; Mahajan, 2010). One lens through which the operation of management and organisations can be viewed is through the study of organisational behaviour.

2.2.1 Organisational Behaviour

Organisations distinctly require humans to achieve objectives and goals, thus the understanding of organisational behaviour is important (Robbins & Judge, 2012). Organisational behaviour evaluates the influences of individuals, groups and organisational structure on the behaviour of an organisation (Martin & Fellenz, 2010). Therefore, organisational behaviour is the discipline focussed towards analysing and understanding the management of organisations, and the reasons behind their operation (Martin & Fellenz, 2010; Robbins & Judge, 2012). Nevertheless, the theories of organisational behaviour attempt to be multi-disciplinary and explanatory in their approach, focussing on the interrelationship of variables, and providing models of thought (Robbins & Judge, 2012; Weissenberg, 1971). Martin and Fellenz (2010) provide a way of dissecting the complexity of an organisation through a structured framework of the micro, meso, and macro lens (*Table 1*)**.**

Table 1. Levels of organisational behaviour analysis (Martin & Fellenz, 2010)

Individual	Micro	Individual	Individual
		Interpersonal	Interpersonal
Interpersonal/Group	Meso	Group	Group
		Organizational	Intergroup
Organizational	Macro	Environmental/Societal	Organizational
			Inter-organizational

This framework provides a number of distinct levels of analysis from which to view the management of organisations. It is important to understand how these levels interact when talking about the way

in which organisations plan, provide leadership, utilise resources and structure themselves (Martin & Fellenz, 2010).

2.2.2 Organisational Structure

The structure of an organisation plays a role in the attitudes, behaviour, and efficiency of staff and the organisation as a whole (Jaques, 1996; Martin & Fellenz, 2010; Robbins & Judge, 2012). An organisational structure refers to the arrangement of tasks, authority and communication relationships, and the influence and control this has on people to co-ordinate and undertake their work (Martin & Fellenz, 2010). Organisational structures can take many forms including; mechanistic, organic, virtual, and bureaucratic, each design having their own strengths and weaknesses (Robbins & Judge, 2012). When organisational structure is considered, it is important to consider the impacts of the organisation size, the technology it implements in its day to day tasks, as well as the environment in which it operates (Robbins & Judge, 2012). These factors can heavily influence the way an organisation operates and is structured.

Whilst there is a diverse set of organisational structures, each have commonality in the core business activities that must be undertaken. Fayol (1949) discussed these core activities as technical, including the production, manufacture, and adaptation of products and services; commercial, including buying, selling, and the exchange of products and services; financial, which is the search for, and provision of capital and its optimum use; security, which allows for the protection of property, persons, and peace of mind; accounting, through which stock take, balance sheets, costs, and statistics are developed; and managerial, which is the provision of organisations and coordination, strategic planning and vision, and command and control is carried out.

Furthermore, Fayol (1949) identifed several principles of management, which Robbins and Judge (2012) assert must be addressed in any organisational structure. These principles include work specialisation, departmentalisation, chain of command, span of control, centralisation, and formalisation (Fayol, 1949; Weissenberg, 1971).

Work specialisation, or the division of labour, is the extent which an activity is broken down into sub-tasks, and how many sub-tasks a worker is assigned to undertake in their day to day work (Robbins & Judge, 2012). For example, factory workers have a high work specialisation, as they are performing the same repetitive task over and over, completing a single sub-task of a greater activity. Departmentalisation is an encompassing form of work specialisation, which groups tasks together, coordinating action through groups or departments (Robbins & Judge, 2012). Commonly, departmentalisation is implemented in alignment to the type of work conducted, the product being produced, the geography or location of staff, or even by the target consumer.

In addition to grouping tasks and delegating this division of labour, it is important to clearly identify the chain of command – the unbroken line of authority throughout the organisation (Martin & Fellenz, 2010). This concept addresses the importance of the delegation of authority to ensure orders can be given and obeyed, whilst maintaining a unity of command, which posits that all workers should have only one direct superior to report to, lest conflicting orders be received (Jaques, 1996; Robbins & Judge, 2012). Unity of command is directly related to the concept of span of control, which outlines the number of employees a manager can control at a time (Robbins & Judge, 2012).

The span of control of a manager directly influences the height and width of an organisation. If each manager is responsible for more staff, the organisation will be wide, but short, allowing for staff costs to be saved, and giving employees more authority, flexibility, and allowing for faster decision making (Weissenberg, 1971). Consequently, the inverse, where a manager controls only a few staff, ensures time is being spent more efficiently, and work is conducted to the expected standard. However this model increases the hierarchy of an organisation, slowing communication down, adding staff costs, and isolating management (Robbins & Judge, 2012).

Furthermore, the principle of centralisation refers to the degree of which decision making is concentrated in an organisation (Robbins & Judge, 2012). The less input management receives from subordinates in making their decisions, the more centralised an organisation is. A decentralised organisation will push decision making authority down the chain of command, allowing for quicker response times, and empowerment of employees (Martin & Fellenz, 2010; Robbins & Judge, 2012).

Finally, the concept of formalisation refers to the degree of job standardisation (Robbins & Judge, 2012). This can relate to the specialisation of tasks where generally, a more formalised role is less complex and very rigid in scope. Roles that are not formalised would be considered more complex due to the freedom of approach and flexibility of goals. Highly unstructured positions would be considered professional or management roles, whilst highly structured roles would be delegated to front line staff (Jaques, 1964, 1996).

Expanding on Fayol's (1949) work, Mintzberg (1980) postulates alongside these core principles and activities, further commonality can be found between organisational forms. This commonality is considered across five underlying roles which include the operating core, the strategic apex, the middle line, the technostructure and support staff (*Figure 1*). Mintzberg considers the central operations of an organisation to consist of the operating core which are the workers who are directly involved in producing the basic products and services of an organisation, or those who directly support their production; the middle line which are those managers who sit above the operating core, providing translation of the strategic goals of the organisation into workable tasks and outputs; and the strategic apex where these strategic goals are created and implemented. Seated alongside these central operations are the analytical workers making up the technostructure; who apply their skills to the design and maintenance of the organisation, adapting it to its environment. The role of technostructure workers is to advise on decision making and other matters (Galbraith, 1985). Finally, support staff, also seated outside of the formal line structure, includes those workers who provide indirect support to the organisation, primarily employed for the exchange of special services.

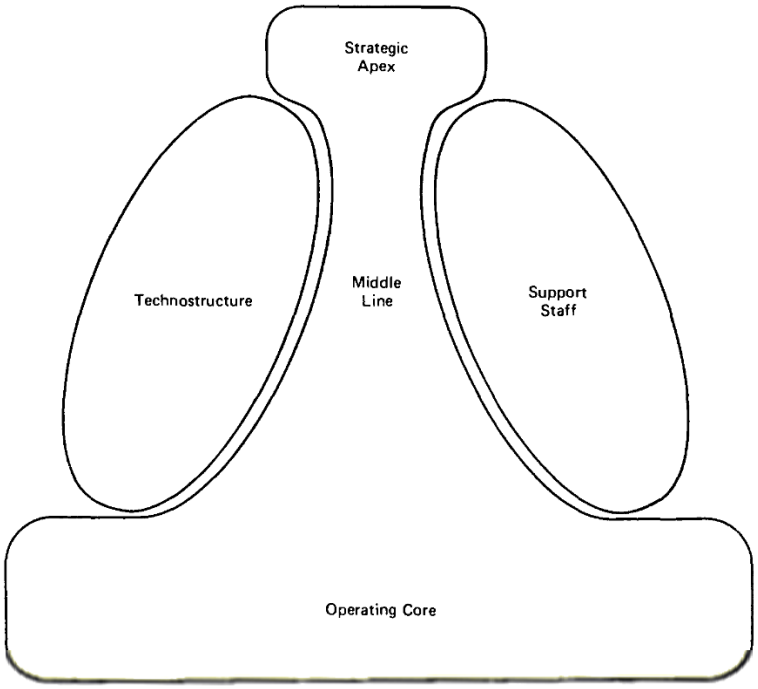

Figure 1. General framework of organisational forms (Mintzberg 1980; Martin & Fellenz, 2010)

2.3 Organisational Management

Martin and Fellenz (2010) argue that an organisation's structure impacts the conduct of work. This impact carries over to the management of staff and the implementation of business functions. Nevertheless, management processes are carried out through a number of central activities such as planning and leadership, and are required throughout the organisation no matter the applied contextual function. Jaques, (1976, 1996) and Mintzberg, (1973, 1980) recognised that managerial work, no matter the functional context, is the central basis for organisational achievement, and these contexts are simply governing relationships of outputs that support business objectives. This view aligns with the behavioural view of management, and ascribes work to process and decision making rather than explicit functions (Mintzberg, 1973, pp. 13-17).

2.3.1 Management Planning

Organisational planning is the core method through which an organisation can achieve its goals and objectives in a structured and coherent way (Mahajan, 2010). The process of planning is multi-faceted, and requires the ability of the planner to objectively forecast the future, whilst utilising the current context of a variety of factors including the external environment, financial information, personnel, customer-client relationships, market conditions and other variables in order to enact an effective plan (Jaques, 1996; Robbins & Judge, 2012).

According to Mahajan (2010), planning is primarily a function of management, and is goal oriented. Jaques (1996) postulated that the process of planning evolves along the stratum of work where complex and long-term plans will be produced by higher strata workers than short-term plans. Nevertheless, Mahajan, (2010) emphasises that planning is a continuous and flexible process, as it is

impossible to successfully predict the future (*Figure 2*). It is considered that the planner must be ready to change the plan according to variable conditions both within and external to the organisation. The outcome of effective planning is the ability to make informed decisions, and plot a course of action to achieve a goal or objective (Martin & Fellenz, 2010; Mintzberg, 1973). Such planning further facilities the reduction of uncertainty within an organisation, and ensures coordination within and between organisational activities (Mahajan, 2010).

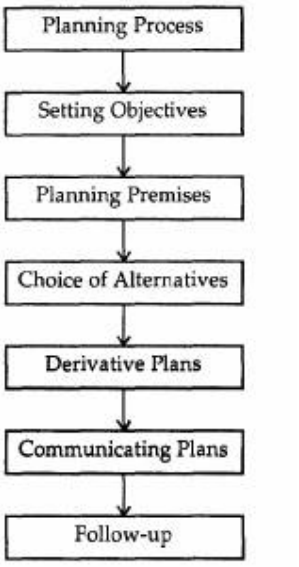

Figure 2. The planning process (Mahajan, 2010, p. 207)

Consequently, the first step in the planning process is to set the objectives and goals of the organisation, and by extension, the objectives and goals of the plan. The second step is to identify and establish any assumptions that the plan will build from. The next step involves identifying a number of alternatives to achieve the goals and objectives outlined initially, which ensures that multiple perspectives are considered and alternative action can be taken if the situation changes (Jaques, 1996).

The main body of work in this process is outlining the derivative plans for the organisation. The core plan outlines the overall goals and objectives for the organisation, whilst the derivative plans include sub-goals, policy and procedures, rules, schedules, and budgets that will outline the roles and functions of activities, departments, and specific jobs throughout the organisation in aid of the core plan (Mahajan, 2010). Once these points have been articulated, the plan must be communicated throughout the organisation, and thoroughly explained to those responsible for its implementation (Jaques, 1996; Mahajan, 2010; Mintzberg, 1973). Finally, a continuous review of the plan must be conducted to ensure it is still viable within the changing context and environment of the organisation (Mahajan, 2010; Talbot & Jakeman, 2009).

2.3.2 Management Leadership

For organisations to achieve their goals, it is argued that effective management and leadership processes must be in place. According to Martin and Fellenz (2010) management is a process that involves the planning, organising, leading and controlling of resources in order to achieve

organisational objectives. However Robbins and Judge (2012) separately define both management and leadership, explaining that management is about dealing with complexity, whilst leadership focuses on dealing with change. Martin and Fellenz (2010, p. 196) further define leadership as a process of influencing others, and facilitating individual and collective efforts to accomplish shared goals. Within an organisation, these roles are not always one and the same. Martin and Fellenz (2010) discussed the importance of followers in influential leaders, and noted that leaders cannot be appointed, they emerge as a situation develops.

These leadership tasks provide the context for management decision making within an organisation (Jaques, 1964, 1996). Effective management and leadership are born out of continual review of subordinates, context, planning and dealing with complexity and change (Jaques, 1996; Martin & Fellenz, 2010; Robbins & Judge, 2012). Mintzberg (1973) outlined roles and responsibilities managerial staff take within an organisation, postulating that all managers are required to take on a mixture of interpersonal, informational and decision roles to be effective. Interpersonal roles consist of the interactions with other people (customers, subordinates, superiors) as a consequence of the type of job held by the manager (Mintzberg, 1973). This includes acting as a figurehead, a leader, and a liaison between the higher echelons of an organisation and the subordinates to the role (Martin & Fellenz, 2010). Informational roles include the way the manager works with information, including the way information is monitored (context), disseminated to the relevant stakeholders, and the way the manager acts as a spokesperson for his role (Mintzberg, 1973). Lastly, decisional roles include the decision making capacity of the manager within the role. As a decision maker, a manager must be able to make entrepreneurial decisions, handle disturbances between subordinates, allocate resources effectively, and negotiate both with superiors, customers, and other stakeholders (Mintzberg, 1973).

2.4 Jaques' Requisite Organisation

Jaques' extensive work (1951, 1964, 1970, 1972, 1976, 1996, 2002) in organisational theory and managerial hierarchies is at the heart of this research project. Jaques developed a theory for the measurement of work and its use in identifying the occupational stratum of work within an organisation. This approach has been used in the study over other theoretical bases due to its explicit measure of work, which has indicated validity in previous research (Craddock, 2002).

2.4.1 Work, Task Complexity, and Human Capability

All organisations require the conduct of work in aid of achieving their goals and objectives (Jaques, 1976, pp. 15-17). Jaques (2002, p. 19) posits that work is a goal directed choice, and is the direct actions one takes to achieve an assignment or task. The type of work conducted and the goals achieved are directly related to the occupational role one fulfils. Jaques explains work in terms of the judgement and decision making one undertakes within constraints such as law, standards of work, policy, and time (Jaques, 2002, pp. 20-21). Finally, judgement is considered decision making without all relevant information (Jaques, 2002, pp. 22-23).

These underlying concepts form the basis for Jaques' discussion surrounding human occupational capability. First, Jaques (2002, pp. 32-44), and others (Boal & Whitehead, 1992; Gould, 1986; Hooijberg & Quinn, 1992; Jacobs & Lewis, 1992; Stamp, 1981) have discussed the types of

information complexity and the ways in which it can be processed in the production of work. There are four identified methods of information processing, including declarative, cumulative, serial, and parallel (Jaques, 1996, p. 22; 2002, pp. 32-44). These methods are considered along six orders of information complexity, which align with the functional time-horizon of an individual (Jaques, 2002, pp. 32-44). Whilst Jaques (2002) explains six orders of complexity, his theory of requisite organisation is only concerned with the third and fourth order complexity categories (Cason & Laurents, 2006). These categories span from day to months to years to decades in time horizon, and encompass all aspects of organisational work. Third order complexity involves 'emblematic' representation of information, where information is processed through contextual and specific situations (Cason & Laurents, 2006). Comparatively fourth order complexity involves deployment of 'concepts' which are not directly tied to contextual and specific situations (Cason & Laurents, 2006).

Jaques (2002, pp. 32-44) emphasises an inherent human capability to understand complexity, and that such understanding matures over time regardless of education or occupational opportunity. This capability is tied closely with the ability for the individual to perceive time into the future, and is a measure of cognitive capability (Jaques, 1964, 1970, 2002).

2.4.2 Measurement of Work

Jaques (1951, 2002) established that the measurement of work within a role can be achieved by identifying the longest task undertaken in a position. The longest task is required to measure the lengthiest time span of discretion where the individual must utilise judgement and decision making during their work without direct oversight. This is known as the time-span of discretion, and is directly attributable to classification and positioning of an individual in the stratum of work. According to Jaques discussion with the manager of the individual is necessary to identify the longest task completion date specified by the manager (not the actual completion date). This information is then verified by the managers' direct superior to ensure consistency. Measuring task completion in this way allows for the identification of an individual's positioning on the stratum of work (Jaques, 1972, 1986).

2.4.3 Level of Work and Task-Time Complexity Measures

According to Jaques, a distinct strata of work can be identified within all organisations. These strata can be determined by observing an individual's time span of discretion (Ivanov, 2011). The time-span of discretion for a task, paired with the complexity of the task, 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).

Such complexity, tied with the individual's time-span of discretion provides an objective measure of the level of work within a role, and allows for unbiased comparison between roles (Jaques 1996). 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 (

Table 2).

Table 2. Occupational stratum of work in organisations (Jaques, 1986, 1996)

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 Workers

Stratum One: Concrete Shaping / Direct Action

Stratum One work consists of concretely illustrated tasks that can be tackled solely through training and procedures (Jaques, 1996). Work at this level carries a prescribed output, with specific circumstances where the application of training and procedures can be carried out. Individuals working at this stratum are not expected to solve problems outside of their prescribed tasks. Where obstacles arise practical judgement and trial and error approaches are expected to be applied by the individual to solve the problem (Jaques, 1996). However, if this process is unsuccessful, workers are expected to seek out a supervisor to provide instruction. Rowbottom and Billis (1977) ascribe this type of work as that which can be reasonably demonstrated once, and applied to various situations.

It is considered that workers that meet the criterion to be classified as a Stratum One role are first line manual workers, clerical workers, and other front-line staff. The time-span of discretion for this role is between one day and three months (Gould, 1986). Decision making and the exercise of judgement comes from the prioritisation of tasks, and the application of the right procedure or training to achieve the tasks specified.

Stratum Two: Diagnostic / Task Definition

Stratum Two work is considered to be first line managerial work, or supervisory work (Jaques, 1996). Nevertheless, Stratum Two tasks do not have a completely specified output, and require interpretation from the individual to achieve the task. This interpretation includes the cumulative collection and processing of information, leading along a linear path of progression, metered by the speed and processing of this data collection (Rowbottom & Billis, 1977; Jaques, 1996). Furthermore individuals at this stratum of work are expected to work on an individual basis, and through a process of self-reflection and forecasting, identify potential problems before they occur in the future.

Whilst a Stratum Two role is still bounded by policy and procedures, the rigid definition of the problem solving process is removed (Jaques, 1996). Judgement and problem solving occur over a time-span of discretion between three months and one year (Gould, 1986), with a functional output that is only partially prescribed. Individuals that fulfil Stratum Two work are generally supervisors, first line managerial staff, specialist professional roles such as engineers, and graduates (Jaques, 1996).

Stratum Three: Task Extrapolation / Alternative Serial Paths

Stratum Three work requires the ability to serially process tasks and manage future obstacles and situations as they arise (Jaques, 1996). Individuals at this level of work must be able to consider the current working environment, develop a manageable plan with alternatives, and meeting short term and long term expectations in the pursuit and achievement of goals. Consequently, work at the level involves developing new systems and procedures which prescribe the way future situations will be handled, and this includes work conducted by Stratum One and Stratum Two workers (Jaques, 1996). Furthermore, work at this level requires direct judgement, paired with diagnostic accumulation of information which encompasses the whole plan, ensuring the capacity to change direction to an alternative path if required across a time-span of discretion of one to two years (Grobler, 2005).

Individuals operating at Stratum Three are generally considered as fulfilling systematic service provision roles such as senior or chief engineers, doctors, and lawyers (Rowbottom & Billis, 1977; Jaques, 1996). Stratum Three managers can employ up to 200-250 people, but cannot create new business units or implement new technological solutions.

Stratum Four: Transforming Systems / Parallel Processing Tasks

Stratum Four work moves beyond direct management tasks and progresses into general management (Jaques, 1996). Consequently, it is expected that workers can develop pathways to goal achievement for multiple situations simultaneously, allocating finite resources between each situation (Jaques, 1996). Rowbottom and Billis (1997) note that Stratum Four individuals demonstrate the ability to meet short term, identifiable needs across simultaneous projects whilst maintaining long term organisational priorities. Furthermore, individuals at this level of work do not set strategic direction, but influence and enact the process of implementing it; aligning with Mintzberg's discourse of the middle line worker (Mintzberg, 1980).

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. 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 constitutes the role of a general manager (Gould, 1986; Jaques, 1996).

Stratum Five: Shaping Whole Systems through Direct Action

Stratum Five work consists of operations at the level of a unified whole system or business unit (Jaques, 1996). Operations at this level are unbounded by the environment and are directly by the executive stratums of work. Individuals working at this stratum must be able to judge the likely impacts or consequences of decision making and events that occur both internally and externally to the business unit (Jaques, 1966). This judgement extends to second or third order consequences in the operating environment. Furthermore, individuals at this level of work are responsible for sensing the inter-connection between tangible and intangible variables within the business unit, and must take direct action to account for these variables.

Work at Stratum Five includes recruitment and training strategies, as well as mapping the business units outputs to the needs of the external market (Jaques, 1996). This role is devoted to acting within a constantly changing external environment, mapping the consequences of these changes internally, and adjusting as required to meet market demands. The time-span of discretion for individuals operating at this stratum of work is between five and ten years (Gould, 1986).

Stratum Six: Defining Whole Systems through Cumulative Processing/Conceptual Abstract

Stratum Six work is considered outside of the unified whole system encountered at Stratum Five, operating entirely externally with considerations to the political, technological, social, economic and intellectual external environments (Jaques, 1996). Consequently, the role involves shaping and influencing these environments in line with the organisations' strategic goals, contributing to the long-term survival of the organisation in the marketplace. Such individuals are required to develop external networks through which diagnostic information can be collected, whilst judging corporate investment priorities over a time-span of discretion of 10-20 years (Gould, 1986).

Nevertheless, Stratum Six work requires a strong capability to cope with change, and chart decision making and long-term strategy across increasingly complex environments (Ivanov, 2011; Lee et al., 2010). Generally, Stratum Six workers are considered vice-presidents in the executive stratum of work, with responsibilities for multiple business units. These responsibilities include assessment and alignment of these business units to the core business outputs and strategic vision (Jaques, 1996).

Stratum Seven: Development of Whole Systems through Extrapolative Development

Stratum Seven work is embedded in the concept of societal needs expressed through the market. Work is abstract in nature, and decision making is always exposed to high levels of uncertainty and complexity (Jaques, 1996). Stratum Seven individuals are required to develop and pursue multiple world-wide strategic plans; conceptualising alternative pathways over a time-span of discretion of over 20 years (Gould, 1986). Furthermore, these plans must be supported through long term, and often internationally sourced, financial resourcing. Consequently, individuals at this level of work must be capable of thinking on an international scale, grappling with the inherent complexity of such a task (Jaques, 1996).

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).

2.4.4 Criticisms of Jaques' Theories

While Jaques' work has endured prominance over many years, in critique of Jaques' (1996) framework, Boal and Whitehead (1992) suggest that in crisis situations, the time-span of discretion in a role compress significantly. They argue that because of this, it could be possible for an individual's time-span of discretion to shift depending on the specific situation that they find themselves in. Consequently, Boal and Whitehead (1992) continue to explain that Jaques' (1996) framework is oriented towards understanding so called ‘tame’ problems. However the application of

the theory breaks down in considering 'wicked' problems, which may not have a foreseeable solution. Furthermore, according to Hooijberg and Quinn (1992) the time-span of discretion measurement is not sufficient to gain a holistic picture of an individual's capacity for work. They argue that an individual's work capacity is in part, aligned to Mintzberg's (1973) discourse on managerial types, alongside other managerial and information processing theories.

Another potential criticism of Jaques' body of work is suggested by Ivanov (2011) who explores the application of Jaques' Requisite Organisation theory to modern organisations, examining the time-span of discretion across various levels of an organisation. This study determined that many modern organisations are operating at a compressed time-span of discretion, which leads to excessive red tape, bureaucracy and inherent mistrust between levels of work. Whilst this finding does not directly dispute Jaques' work, it could suggest that the application of his theories to modern organisations may require further research, specifically in the delineation between strata and the time-span of discretion measure. Further evidence of this potential misalignment in modern organisations is suggested by Stichweh (2008) and Rossi (2008), who assert that the globalisation of society has significantly reduced temporal-spatial considerations, alongside compressing societal structures and stratums. Contrary to this argument however, is significant support in the literature for the time-span of discretion measure, alongside various studies examining Jaques' body of work (Craddock, 2002).

2.5 Corporate Security

Sitting within the corporate strata of organisational activities is the corporate security function. Fayol's (1949) early organisation theory considered security as a fundamental organisational activity to achieve business goals. Nevertheless, as the function has evolved and grown over time the discipline has broadened significantly, with applications 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 contested, with many agreeing that the concept of security is contextual, and as such, difficult to define (Cubbage & Brooks, 2013; Fay, 2002; Fischer, Halibozek, & Green, 2008; Hillman, 2011; Prenzler, 2005). Regardless, the concept of security can be considered from the individual, group, and national context, each with their own implied assumptions, meanings, and applications (Smith & Brooks, 2012, p. 7).

Fischer et al. defines security as "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" (2008, p. 31). This definition explores the broader objectives of any security system or approach across the domain. Fischer clarifies that security is the method through which individuals and groups, including organisations, governments, and societies can progress their own goals without disruption. However, this captures elements of the safety domain into its definition of security; a distinction of importance. Significantly, Talbot and Jakeman delineates this distinction, and defines security as "the condition of being protected against danger or loss. It is achieved through the mitigation of adverse consequences associated with the intentional or unwarranted actions of others" (2009, p. 5).

The specific consideration of the adversary or threat vector, alongside the explicit outline of the intentional action of others ensures a differential from safety concerns. Furthermore, Somerson (2009, p. 51) highlights this delineation between security and safety by defining security as an approach to protect against felonious acts of others, whereas safety is an approach to protect against the duncery of negligence. This boundary of responsibility resonates with Fayol (1949) who defined security as the protection of property and persons, and delivering peace of mind. The inclusion of intent in Talbot and Jakeman's definition in an important one, as security mitigation strategies are considered from the perspective of preventing a rational actor (Clarke, 1995; Garcia, 2006, 2008). Garcia summarises by defining security as "systems used to prevent or detect an attack by a malevolent human adversary" (2008, p. 2).

Through examination of these definitions and considering the contextual nature of security, the working definition of security for this thesis will be

> "The protection of individuals, groups and property through systems designed to mitigate danger or loss from a malevolent human actor."

2.5.1 The Practice of Security

Security is primarily about the protection of individuals, groups and property. Such protection is implemented though specific systems and processes that combined aim to mitigate danger and loss (Fischer et al., 2008). These systems focus on the aspect of threat, rather than the aspect of a hazard which is the core differential between security practice and safety practice (Somerson, 2009). Coole, Brooks and Treagust (2015) suggest that security practitioners operate through a process of diagnosing the problem, inferring the cause, and applying treatment to the problem using protective security measures. Consequently, the practice of security consists of three cumulative phases, each drawing on an underlying and abstract body of knowledge (Smith & Brooks, 2012).

Security Diagnosis

Coole, et al. (2015) discusses the concept of security diagnosis as the process through which a security practitioner determines the security problem within a context. Accordingly, the practitioner reviews and analyses available information about the problem, revealing conditions which require intervention to reduce security risk. This process includes identifying relevant legislative, regulatory, and governing frameworks in which the organisation operates (Talbot & Jakeman, 2009), conducting a security survey (Fennelly, 1997), and characterising the facility (Garcia, 2008). Consequently, through this process of determining, discovering, and identifying (Abbott, 1988, p. 229), security practitioners are able to ascertain the threats to the organisation, and consider the appropriate measures of control.

The concept of a security threat is the core driver behind all security practice (Brooks & Smith, 2012). A security threat stems from an underlying root cause such as sociological factors that cannot be mitigated through simple security system design. These factors are generally targeted by government policies, law, and other intervention strategies (Brooks & Smith, 2012; Standards Australia, 2006). According to White, Haines and Asquith (2012), underlying factors can cause strain on individuals and groups, and this manifests itself in deviance from the norm of society. When this deviance is targeted at an asset of security concern, it becomes a security threat; a malevolent human actor who has the intent and capability to pose a risk (Garcia, 2008).

Such a human has the potential to originate from inside an organisation, outside an organisation, or through collusion of these two parties (Garcia, 2008, p. 29). These three threat vectors must be tackled in fundamentally different ways, as the capabilities and access of each are fundamentally different. Garcia (2008, p. 29) suggests a mixture of physical protection systems, material accountancy and material control to cover the breadth of this threat spectrum. These control considerations are reasoned through the security inference phase of professional practice.

Security Inference

The security inference includes the use of knowledge and judgement to articulate the requirements for an effective treatment solution to the diagnosed security problem. Consequently, the problem complexity plays a significant role in the level of inference required by the practitioner about the source of the problem, and the appropriate strategies used to counteract the identified threat (Coole et al., 2015). Furthermore, the inference phase requires the practitioner to draw from an abstract body of knowledge to underpin reasoning and decision making. Such an abstract body of knowledge could include concepts such as the theory of rational choice and routine activity theory (Cohen & Felson, 1979), situational crime prevention (Fennelly, 1997), crime prevention through environmental design (Atlas, 2008), and systems theory (Coole, 2010).

Security Treatment

Once the security practitioner is satisfied with their understanding of the security problem (threat) and its cause and probable evolution (application of an underlying theory), the security treatment phase begins. This phase generally considers the application of minimum compliance with legislation and regulation first, with an appreciation for duty of care (Garcia, 2008; Coole et al., 2015). In addition, an application of security risk management frameworks alongside the planning and design of physical control measures is undertaken (Standards Australia, 2006; White, 2014). Such planning and design must consider the underlying concepts of deter, detect, delay, respond, and recover (Garcia, 2008; Coole, Corkill, & Woodward, 2012) to ensure all implemented strategies are achieving key security outcomes within a concept of defence in depth and a holistic approach to security (Smith, 2003; Nunes-Vaz, Lord, & Ciuk, 2011). These security elements and design decisions come together to treat the security problem through the achievement of environmental control and risk mitigation.

2.5.2 The Corporate Security Jurisdictional Boundary

In the application of these underlying theories and practice, Brooks and Smith (2012) suggest corporate security is responsible for issues arising in the peer, group, organization, and community spheres of the broader security domain. Such responsibility leads to an interesting interplay of authority, specifically those of security management, risk, the built environment, and core security principles such as defence in depth, situation crime prevention, and crime prevention through environmental design (Fennelly, 1997; McCrie, 2001; Sennewald, 2011).

According to Abbott (1988), professions have jurisdictional boundaries that must be defined to ensure scoping of work, and Fayol (1949) has delimited organisational functions into essential activities of practice. Accordingly, Fayol (1949) identified corporate security as one such group of essential activities, with a delineated boundary of work. This boundary however, must be placed in context to ensure understanding. Sarre and Prenzler (2000) and Prenzler (2005), discuss the

delineation between private and public security services. They argue that public security services are responsible for policing and enforcement tasks, whilst private security is responsible for the rendition of protection services (Prenzler & Milroy, 2012; Prenzler, Sarre, & Earle, 2008; Sarre & Prenzler, 2000).

This discussion is further elaborated into the differences between private and corporate security; where private security practitioners are focussed on the provision of contracting services, and corporate security practitioners render in-house services to organisations (Prenzler, 2005). As argued by Brooks and Smith (2012), there is significant overlap between the private and corporate practitioner in terms of their applied context, with both jurisdictions having authority at the community, organisation, group, and peer levels of security application.

According to Wilensky (1964) a profession must have a clearly defined body of knowledge, and professional authority to exclude those who do not meet the criteria of a practicing professional. Security, does not yet meet this criteria (Brooks, 2013; Griffiths et al., 2010). However, professional practice can still be conducted by practitioners in the field (Talbot & Jakeman, 2009; Wilensky, 1964), that is individual practitioners can be professional. Consequently, through the use of a professional theory, development of a working definition of corporate security can be achieved. It is argued that corporate security is a practicing domain of security, where the applied practice is considered security management, which Fayol (1949) argued is a core activity of any organisation (Fay, 2002; Sennewald, 2011).

Therefore, the working definition of corporate security shall be defined as the systematic framework of controlled organisational security through the mitigation of risk against assets, people, and information through technological, physical, and procedural controls (Smith & Brooks, 2012; Coole, 2010; Fennelly, 1997; Fischer et al., 2008; Garcia, 2008; Griffiths et al., 2010; Talbot & Jakeman, 2009).

Finally, the applied practice of corporate security, herein referred to as security management, shall be defined 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 (Smith & Brooks, 2012; Craighead, 2009; Cubbage & Brooks, 2013; Fischer et al., 2008; Talbot & Jakeman, 2009).

This definition firmly places the security function within organisational practice and embeds security outputs within organisational goal setting and achievement. It is important to consider security management as simply an applied management context, where generic managerial skills are utilised to inform specialised security practice (Fay, 2002; Fayol, 1949; Mintzberg, 1973; Sennewald, 2011).

2.5.3 Corporate Security Roles and Functions

The corporate security function, generally being the provider of in-house security services to organisations, has many roles and responsibilities. Due to the ambiguity that surrounds corporate security practice, and its lack of a clear definition, the literature suggests a broad and varied set of roles that construct the corporate security domain. Prenzler (2005) delineated the corporate security function from private security through the delineation of in-house services and contract

services, which has provided a starting point for role definition. Barefoot and Maxwell (1987), Smith and Robinson (1999), Fay (2002), the Interim Security Professional's Taskforce (2008), Sennewald (2011) and Brooks and Corkill (2014) have further elaborated on what is considered the stratum of work in the corporate security industry, alongside perceived roles and functions.

Barefoot and Maxwell (1987) argues for the corporate security practitioner to be a business manager first, with consideration for the security specialisation second. They argue for the function to have the ability to probe all areas of the corporate organisation to ensure compliance with policy and procedure, alongside consideration of inter-departmental assets. Emphasis is placed on the corporate security manager being a loss prevention function, and consequently, the corporate security manager should work on the premise of prevention and control, with the end goal being the reduction or elimination of loss (Barefoot & Maxwell, 1987, pp. 6-7). Nevertheless, four differentiated strata of work within the corporate security function are identified; those being the staff investigator, the chief investigator, the regional security manager, and the security director (1987, pp. 195-198).

These four functions are delineated with various roles and responsibilities. The staff investigator is expected to work alone in the conduct of investigations, and have a strong specialised knowledge in law enforcement techniques. Accordingly, this role reports to the chief investigator, who has responsibilities that include; recruiting, hiring, training, and supervising staff investigators, and assisting in major investigations. This role is functionally seated below the regional security manager, whose responsibilities span security surveys, the review of systems and procedures, the monitoring of lower stratum functions. Finally, at the apex of the corporate security function according to Barefoot and Maxwell (1987), is the security director, whose responsibilities encapsulate all persons seated below the role, alongside the strategic steering of the function to align with business objectives.

Following this examination of the corporate security function, Smith and Robinson (1999) articulate the corporate security stratum of work to include those individuals who can apply functionally different competencies in their work (*Figure 3*). The apex of this stratum is considered to be the security manager, who is considered to be an executive with the responsibility to assess and mitigate security risk, and in so doing, protect the assets of an organisation. Operating below this strata of work are security technologists, who consists of scientists and engineers who develop security systems to protect the assets of an organisation. Security technicians provide services to install and maintain security systems and equipment; where security guards have responsibility for the maintenance of order, the enforcement of rules and procedures, the provision of access control, and the protection against loss from fire and equipment failure.

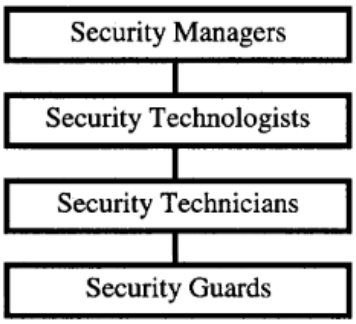

Figure 3. The corporate security stratum of work (Smith & Robinson, 1999, p. 30)

Juxtaposed to Smith and Robinson's discussion, Fay (2002) explores the corporate security manager's roles and responsibilities, but does not elaborate on the stratum of work. Fay's approach is very operational in its explanations, and does not truly articulate a deep appreciation for the corporate security function. Interestingly, the only identified corporate security roles in this body of work are the security manager and the security officer, leading to the conclusion that this text could arguably be considered a supervisory handbook.

Prenzler (2005) in his examination of the Australian security industry, explored the Australian Bureau of Statistics (ABS) 'security provider' classifications for census data (*Table 3*). These roles, according to an alignment with Jaques (1996), would be considered Stratum One or Stratum Two roles. Significantly, according to Prenzler, the census data does not collect specialist data on corporate security practitioners outside of these classifications.

Table 3. Security roles as outlined by the Australian Bureau of Statistics (Prenzler, 2005)

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

Building from this discourse, and contrary to Fay's (2002) discussion, the Interim Security Professional's Taskforce (2008) articulated six strata of work with delineated boundaries of work and roles of authority (*Figure 4*). In consideration of these roles, a list of activities, responsibilities, training, and interfaces were provided, each with a functional time span attached. The Interim Security Professional's Taskforce articulation of these roles uniquely defines the core operations of the corporate security function, and provides a comprehensible stratum of work.

	Chief Security Officer	Security Manager	Security Operations Manager	Supervisors	Shift Leaders	Security Staff
	STRATEGY		OPERATIONS		TACTICAL	
	Strategy and Planning		Implementation and Development		Compliance and Operations	
	1 to 3 year	< 12 months	< 3 months	<30 days	1 to 3 shifts	Less than duration of one shift
Activities	Strategic Planning & Sec Mgmt Systems Performance Agreements Stakeholders	Quality Assurance Assessment of systems	Rostering Analysis of activities (Eg: GCS, Supervisor Activity Plans, Compliance with SOP's)	Oversight day to day operations Liaison at local level	Facilitate smooth operation of security activities Security audits Conduct QA checks and remedial training Staff duties as required	Access Control Customer Service Emergency response, disaster recovery, business continuity Troubleshooting Security taks (patrolling, sysadmin, etc)
Responsibilities	Standard Setting	Standard development and implementations	Ensure consistency of operations across all sites and all shifts	Ensure security staff work to Standards & SOP's Monitor maintenance and administrative activities Implement and report on Group plans	Leadership of operational units Ensure compliance with standards	Compliance with SOP's Personal discipline and presentation Knowledge of SOP's
Training	Approval & resourcing Training Plan Briefings to Supervisors Delivery of strategic and specialist training	Development and updating Training Plan Maintain Training Register and monitor plan for compliance Monitor Quality of Trg	Coordinate training activities Develop training materials Ensure logistics and competent instructors	Train large groups Develop training material and aids	Train small groups and one on one OJT Contribute to development of training program	Participate in training Feedback & Improvement suggestions to trainers Personal training and development at posts and in own time
Interfaces	Division Heads and C-Suite Senior external groups (Government, Senior Law Enforcement Officials, etc) Suppliers & Contractors	Regional external Groups (Regional Police and Government officials and group, etc) Internal middle management	Local external groups (Police, Community groups etc)	Supervisors in other departments and contracting companies Administrative personnel	Day to day follow up of tasks with supervisors and admin personnel from other internal groups	Customers, clients and visitors to site

Figure 4. Corporate security roles and responsibilities (Interim Security Professional's Taskforce, 2008, p. 31)

In juxtaposition of this viewpoint, Sennewald (2011, pp. 55-72) suggests that the lower tiers of an organisation consist of general security officers and employees. These individuals operate as the face of the department to other departments, and directly impact the organisations holistic view of the security function. Sennewald argues that security employees at this level are service oriented, with direct interaction with other staff members and the general public. Furthermore, Sennewald (2011) postulates a security supervisor whose responsibilities span hiring, training, disciplining, motivating, promoting, and communicating with security staff. Consequently, the security supervisor is required to act as the key communication link between the security management layer of an organisation and the operational layer, effectively organising the workforce to achieve managerial goals.

The highest tier of a corporate security function according to Sennewald (2011, pp. 43-53) is the security director. This role encompasses responsibilities for the development and implementation of security policies, advisement on security related issues, risks, and threats, and strategic direction and trend setting for the function and the organisation at large. Sennewald argues that the security director must be technical specialist with some appreciation for broader managerial skills and concerns.

In consideration of these roles and functions, Brooks and Corkill (2014) suggest that individuals operating at the lower stratum of security work in organisations must be technically adept, and heavily restricted in their scope of work (*Figure 5*). They suggest individuals operating as a front-line security manager should be responsible for providing security advice, and aligning security policy with broader corporate policy within the context of a single site. The manager at this level of work is responsible for the implementation of security procedures; using highly technical skills, analytical thinking, and specialised techniques.

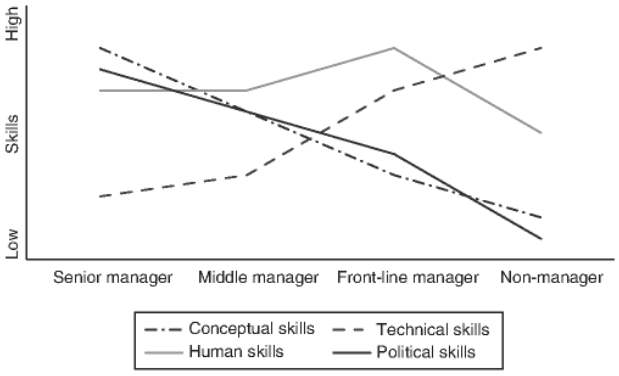

Figure 5. Managerial and technical skills in work (Brooks & Corkill, 2014, p. 222)

Furthermore, Brooks and Corkill (2014) identify a middle level managerial role within the stratum of corporate security practitioners. This role begins to shift from the application of purely technical skills to the application of generalist managerial skills. The security manager at this level of work is responsible for the provision of threat and risk analysis to business units across the organisation. Brooks and Corkill (2014) suggest that security is applied internally in this role through policy and procedure, alongside investigation where required.

The senior security executive as identified by Brooks and Corkill (2014) is focussed on security governance and the achievement of strategic organisational goals through the application of

security. It is argued that individuals working within this classification have functional responsibilities encompassing multiple business units, such as the security, safety, and facility management departments. The executive is involved with shaping internal and external influences to achieve strategic goals, and in doing so, produces and disseminates vital security intelligence, and security risk management across the organisation. In agreement with this discussion is Bayuk (2010) and Cubbage and Brooks (2013), who argue that security management should be championed at the executive level of work, with influence on strategic decision making.

In consideration of these broad perspectives, it is clear that there is a distinct lack of consensus amongst the corporate security literature in the articulation of a stratum of work. That is, there is a significant overlap in some areas of discussion, and disconnects in others. Through appreciation for these bodies of work, the study explores the stratum of work from an external, outsider's perspective, adopting the socio-organisational literature as grounding for the investigation into the stratum and seating of the corporate security function within the corporate enterprise.

2.6 Conclusion

The chapter presented an overview of the literature informing this study, orienting and grounding the reader's understanding of the thesis. In summation, the theory of structural functionalism provides for the differentiation and stratification of society, and identifies an occupational stratum of work. Embedded within this literature, Jaques (1996) expounded a general theory of management, which provides for the exploration of this stratum of work within organisations. This body of work articulated seven strata of work, each with clear and delineated boundaries. This theoretical frame provides a basis for the discussion of managerial skills such as planning and leading in the context of specialised activities such as accounting, financial and security. Such activities can be classified into three general roles within the organisation; those being the technostructure, support staff and operating core. Further informing the study was due consideration to the expansive corporate security literature, with an extensive review of the underlying principles and theories of applied security, as well as an exploration of the variated corporate security stratum of work. Consequently, through a sociological grounding and robust analysis of the literature, the study can be designed to provide a holistic uncovering of the corporate security function within organisations.

CHAPTER THREE: METHODOLOGY

This chapter presents the research methodology, which articulated the study design, the chosen population and sample, the analysis framework, and ethical considerations. The theoretical foundation of the study lies within structural functionalism (Dillon, 2013; Durkheim, 1984; Wilensky, 1964), and its philosophy of research within ethnography (Creswell, 2009, pp. 13, 16; Fetterman, 2008). Consequently, the study draws on qualitative research designs. Ethnography is the description of a group or culture, which is identifiable through shared behaviour, knowledge, and beliefs (Fetterman, 2008). In a pragmatic search for truth, ethnographic principles were used to inform the study design and ensure consistency with the underling theory. As Creswell (2009, pp. 10-11) argues, the use of multiple measures and world-views are vital to ensure validity and reliability of results in qualitative research (Creswell, 2009, pp. 10-11).

3.1 Study Design

The study was grounded in the research philosophy of ethnography, and was conducted in two stages. First, an examination and critique of the literature and underlying theory was conducted to develop a valid research instrument. This instrument consisted of two tools, the Work Measurement Scale (WMS) and Task Complexity Measurement Tool (TCMT), combined into an online survey questionnaire. This questionnaire was then distributed in the second stage to the participant sample (Section 3.3). Subsequently, the survey results were then analysed, with findings presented from the context of the research questions (Chapter Five), leading to the discussion and interpretation of such findings (Chapter Six and Seven).

3.2 Pilot Study

The pilot study provided researchers with an avenue to explore a phenomenon under examination before committing to a full scale research project. The study sought to use a pilot study to ensure the methodology and data collection instruments were sound before committing to the full scale main study. This pilot study was conducted (Chapter 4), and it provided guidance for the conduct of the main study.

3.3 Population and Sample

When conducting research the determination of a suitable research sample, as discussed by Cohen et al. (2007, p. 143), is dependent on the population that the research is attempting to understand. Factors such as time-constraints and the nature of the research must also be considered when determining sample size for research (Cohen et al., 2007, p. 143). In light of research scope, for the pilot study, the population of Western Australia was considered. In 2014 this population consisted of 2, 589, 100 people (Australian Bureau of Statistics, 2014). Narrowing this population down to increase relevance, Prenzler (2005) found that the Western Australian security population consisted of 762 security installer licenses, 812 consultant licenses, and 517 security agent licenses, for a total population of 2091. Considering this, a non-probability sample was chosen as it aligns with the

nature of the study and the inherent nature of ethnographic approaches to research (Cohen et al., 2007, pp. 151, 155; Fetterman, 2008).

For the main study a broader population consisting of international security practitioners was considered. According to the Australian Security Industry Association (cited in Brooks, 2013, p. 1), in 2008 the Australian security industry employed over 150, 000 security personnel. Furthermore, van Steden and Sarre (cited in Prenzler, Earle, & Sarre, 2009, p. 2) suggest that in 2004, the population of security personnel in the European Union had increased to over one million practitioners. Such large populations hinder the collection of a statistically valid sample, and as such, a non-probability sample was also chosen from practitioners located in the European Union and Australia for the main study.

3.3.1 Sample Frame

The sample frame for this study requires participants to:

- Be a security industry practitioner;
- Be of any age;
- Be of any nationality;
- Hold any position regardless of seniority;
- Hold any experience in the industry;
- Hold any level of formal qualification (none, certification, degree).

This frame ensured scope limitations, whilst allowing for a broad mixture of respondents. As the study was attempting to measure the stratification of work across the entire security industry, it is vital that restrictions are limited.

3.3.2 Sample Selection

Sample selection was undertaken purposively, through snowball sampling (Cohen et al., 2007, pp. 156-160). This was achieved through the identification of key individuals at different perceived levels of work who have been determined as gate-keepers across the industry. The initial selection of participants were considered with the goal of penetrating as many levels of work within organisational hierarchies as possible, as some of the members of this sample are in hard-to-reach groups (Cohen et al., 2007, p. 158). Further, through the use of snowball sampling, the survey was able to reach more potential respondents than otherwise possible, and potentially individuals outside of the identified population whom still meet the sample criterion (Cohen et al., 2007, pp. 158-159). The requirement for a statistically valid sample was not considered here, as the research was exploratory in scope, aiming to uncover the usefulness of undertaking such an approach to the research. Hence, given a population size of 2091, a non-probability sample size of 40 was proposed.

3.4 Instrument

The research instrument was developed as an online survey that includes two measurement tools. These tools are the Work Measurement Scale (WMS) and the Task Complexity Measurement Tool (TCMT). The instrument was designed to gather cross check information first, followed by the implementation of the two tools.

3.4.1 Work Measurement Scale

The Work Measurement Scale (WMS) examined participants' current level of work through an examination of the longest task or tasks being conducted into the future. Participants were asked a series of questions about different aspects of their work, aligned to the managerial types identified by Mintzberg (1973). These managerial types were then articulated along a scale that is aligned with the time-span of discretion measure postulated by Jaques (1996). Participants were asked how far into the future they conducted various aspects of their work, with groupings of responses across time-span being considered an indicator for that individual's level of work.

3.4.2 Task Complexity Measurement Tool

The Task Complexity Measurement Tool (TCMT) provided a measure of the task complexity of an individual's work role. This measurement was achieved through a Likert Scale, with a series of questions pertaining to the participant's conduct of work. The strongest agree statement was an indicator of the task complexity in the participant's role. This instrument was directly adapted from a tool utilised by Jaques in his exploration of organisational work (1996, p. 72).

3.5 Analysis

The survey instrument design incorporated ordinal and interval data measurement through the utilisation of two separate measurement tools (Fowler, 2014, p. 86). The Work Measurement Scale (Appendix A) identified an individual's stratum of work by examining different aspects of their role along a scale of time posited by Jaques (1996, pp. 41, 64-71). The longest rated task, or groupings of tasks, will indicate the individual's stratum of work (Jaques, 1964, 1972). The Task Complexity Measurement Tool (Appendix B) provided a measure of an individual's work through perceived task complexity (Jaques, 1996, p. 72). The strongest agreed upon statement will be used to identify the task complexity within the individuals working role. These two tools were enveloped in the overall online survey instrument (Appendix C), which asked a number of grouping questions to aid analysis informing the response to the study's postulated research questions.

3.5.1 Reliability and Validity

The instrument developed in this study was measured for internal consistency as a form of reliability alongside the idea of equivalent-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 were considered through cross tool averages and standard deviation. This measurement did provide insight into the instruments ability to cross check across tools, and ensured an understanding of the instruments capability to measure the work construct. Through implementation of two tools in aid of measuring the same construct, equivalent forms reliability and internal consistency were satisfied through score correlation (Christensen & Johnson, 2014, pp. 168-169).

Validity in questionnaire instruments is determined by the accuracy of the inferences or interpretations one makes from the test scores (Christensen & Johnson, 2014, p. 165)**.** In order to be valid, a questionnaire requires many types of validity measures, including; content, construct and face validity (Cohen et al., 2007, pp. 213-214). Content validity refers to the measure of a test's

relevance to measuring a particular phenomenon (Cohen et al., 2007, p. 213). Content validity was initially tested through face validity. To ensure face validity in the study, the constructed instrument was analysed and judged by two security academics. The instrument design was further honed over time to ensure relevance.

Construct validity refers to the questionnaire items' indication of the underlying theory or phenomenon being measured (Cohen et al., 2007, p. 123)**.** The development of the survey instrument in this study was grounded in the underlying theory of Jaques' requisite organisation, and the general management literature (Brooks, 2013; Brooks & Corkill, 2014; Smith & Brooks, 2012; Griffiths et al., 2010; Jaques, 1964, 1970, 1972, 1976, 1996; Mintzberg, 1973, 1980). Survey questions were directly drawn from themes and measurement tools developed in this literature.

Furthermore, both content and construct validity were supported by the use of two independent measurement tools in the survey. Each tool analysed a different measure of work stratification, both of which are indicators that can be self-confirmation measures.

Finally, face validity is a measure that the instrument measures what it purports to measure (Cohen et al., 2007, p. 214). It is a type of construct validity, however it can be achieved through a face-value test of relevance (Cohen et al., 2007, p. 214). Again, the instrument was examined by two security academics who agreed that the test appeared to measure what it aimed to measure, thus achieving face validity.

3.5.2 Triangulation and External Audit

Triangulation

Denzin (1989, p. 234) states that qualitative researchers should seek to examine a problem from as many methodological perspectives as possible to ensure a more accurate measure of the truth. Denzin (1989, p. 235) further posits that this approach; triangulation, should be conducted due to research methods in qualitative studies being capable of impacting the environment they are attempting to measure, limiting the effectiveness of one measurement approach (Creswell, 2009, p. 191). In response to this, and to ensure a more effective measure of truth in reality, this study undertook a limited within-method triangulation approach (Denzin, 1989, pp. 243-244). The method employed by this study uses a survey for data collection, and in support of triangulation; two measurement tools were included in the survey. By measuring perceived task complexity alongside longest-task time, triangulation can be achieved. Whilst this is not the strongest form of triangulation according to Denzin (1989, pp. 243-244), it does provide some assurances in the reliability of the study (Creswell, 2009, p. 191).

External Audit

Another measure of reliability and validity in a qualitative study can be through external audit of the methodology, instrumentation, and data collection tools (Christensen & Johnson, 2014, p. 301). Through external, expert critique, methodology and instrumentation can be honed to better suit the scope and direction of the study (Christensen & Johnson, 2014, p. 308)**.** The study utilised two security academic experts in aid of ensuring methodological consistency, instrumentation validity, and overall study reliability in seeking out the truth.

3.6 Research Ethics

In aid of ethical research, all aspects of the study was discussed upfront, ensuring total understanding of participants concerning their obligations, rights to withdraw, confidentiality and anonymity. Further, participants were required to provide consent before undertaking the survey, and were under no obligation to complete the survey once consent was given. All respondents were aware of the voluntary nature of their participation. To ensure an ethically robust study, ethical approval was sought by the Edith Cowan University's ethics committee.

3.7 Conclusion

This chapter presented the study design and methodology in line with the literature on ethnographic qualitative study. The chapter presented how the study achieved its outcomes and responded to the research questions. Consequently, through discussion of the population and sample in Section 3.2, a sample frame was developed to identify those relevant to achieving the research aims. Throughout Section 3.3, validity and reliability concerns were addressed specifically with the survey instrument and the overall study design. Section 3.4 outlined ethical concerns with the research and their management strategies. Furthermore, the chapter presented the conduct of a Pilot study further outlined in Chapter 4, and indicated its need in testing and refining the research methodology and survey instrument for the main study.

CHAPTER FOUR: PILOT STUDY

Chapter Four presents the pilot study conducted to test the methodology and survey instrument. The pilot study consisted of a number of security practitioners (N=16) across the stratum of work who were selected through a purposive, snowball sample. This chapter presents the analysis of the first stage data in response to the research questions. Furthermore, the analysis is then compared to the literature, providing an interpretation of the results. Consequently, the chapter presents the implications these results have to the main study, including required alterations to the data collection instrument.

4.1 Pilot Study

A pilot study provides researchers with an avenue to explore a phenomenon under examination before committing to a full scale research project. Significantly, the pilot study allows researchers to use a small scale version of their proposed methodology on real participants (Martin, 2008, p. 135). The aim of this process is to provide the researcher with an understanding of how the proposed methodology works in practice, allowing alterations in data collection techniques and trialling the analysis process before committing to the full scale project (Martin, 2008, p. 135). Consequently, the pilot study is a useful tool for providing insight into the phenomena under study, allowing the researcher to consider potential interpretations and implications of the results.

4.2 Participants

The participants for the pilot study were selected purposively through personal and professional networks and were known to the researcher and the research supervisor (Section 3.2). The Pilot study was deliberately kept within a closed network to control the targeted levels of work across the sample, ensuring a robust penetration rate. Each individual was asked to forward the survey to one other known person who met the study criterion (Section 3.2).

4.2.1 Response Rate

In total, approximately 100 participants were selected to undertake the survey. The researcher and project supervisor contacted 50 participants who were assumed to have sent at least one email to another participant as requested. Of these 100 individuals a response rate of 16 was achieved. Nevertheless, according to Cohen et al. (2007, p. 286) and Fowler (2014) internet survey response rates can be as low as 10%; and with the achieved 16% response rate, the pilot study exceeded this prediction. Of these 16 responses, only nine were assessable, with three non-responses.

4.3 Response Data

The data received by the pilot survey was tabulated for analysis (*Table 4*). Then responses were assessed, including the assessment of the Work Measurement Scale (WMS), Task Complexity Measurement Tool (TCMT) and Assessed Level of Work. Moreover, the Job Level, Number of Employees Managed, and Job Title responses; which are participant selected for cross check purposes.

Table 4. Tabulated pilot study survey response data

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work
Stratum II					
Not Assessed	27	II	II	VI	II
Precinct Security Manager	20	III	II	VI	II
Manager Operations	150	IV	II	VI	II
University Security Manager & Crisis Team Coordinator	80	IV	II	VII	II
Stratum III					
Manager Campus Services	30	III	III	VI	III
Senior University Lecturer	6	II	IV	III	III
Security Operations Manager	32	III	III	VI	III
Manager Security & Emergency Control Co-ordinator	23	III	II	VI	III
Stratum IV					
Manager Security Operations	75	IV	IV	IV	IV
Not Assessable					
Not Assessed	75	III	IV	Not Assessed	Not Assessed
Security Coordinator	16	III	Not Assessed	Not Assessed	Not Assessed
Not Assessed	Not Assessed	II	IV	Not Assessed	Not Assessed
Security Officer	0	I	III	Not Assessed	Not Assessed

4.4 Analysis

Analysis of the data was conducted where groupings of responses were considered an indicator of an individual's level of work (Section 3.3). Consequently, each response was assessed, with the final assessed level of work score judged with regard to the control questions, overall TCMT and WMS results, and cross check measures such as job title, identified work level, and number of employees managed. Consideration was also given to incomplete responses as they provide insight into the survey construction which aligns to the purpose of the pilot study.

Analysis of the pilot data indicated that the stratum of security work within the corporate organisation spans from Stratum Two through to Stratum Four (*Figure 6*). Furthermore, there is a limited job title alignment across each strata; with the number of employees managed at each stratum varying widely. This employee count for each stratum is as follows: Stratum Two 69 employees, Stratum Three 23 employees, Stratum Four 75 employees (*Table 4*).

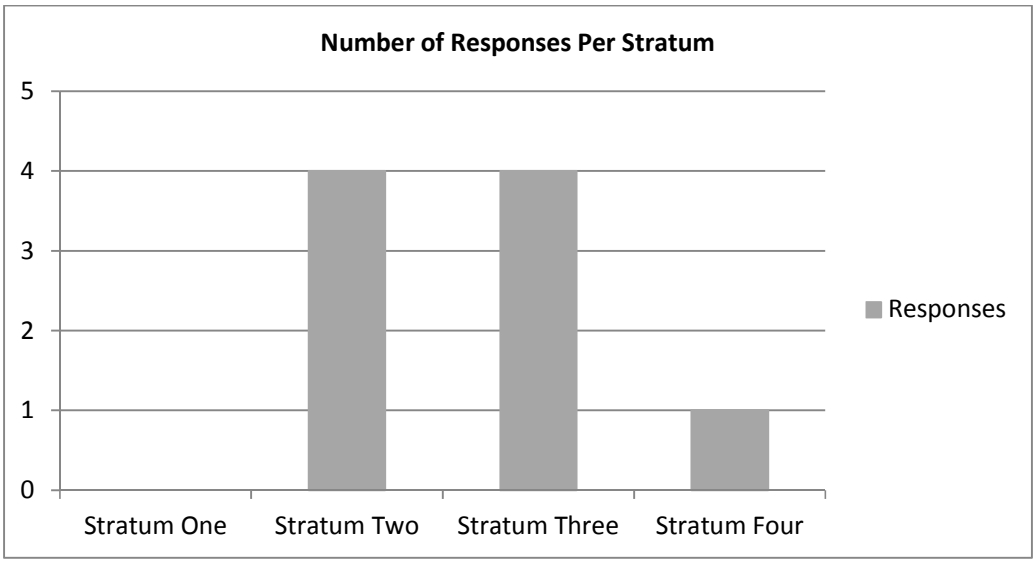

Figure 6. Pilot Study: Number of Responses per Stratum

4.4.1 Assessed as Stratum Two

The analysis of Stratum Two responses indicate four respondents (44%) meeting this criteria. Respondents in this category seemed to overstate their job level initially, but through analysis of the data, especially in the WMS result, enough insight was provided to determine the level of work to be comparable to a Stratum Two individual.

Such individuals are those who engage in tasks that require interpretation to achieve an output that cannot be wholly specified by a superior (Jaques, 1996, p. 66). Consequently, Stratum Two work is prescribed to some extent, but requires individuals to collect information about a problem to provide an adequate solution.

4.4.2 Assessed as Stratum Three

According to the analysis, four respondents (44%) were assessed to be Stratum Three. Respondents identified at this level of work tended to have an accurate picture of their role and responsibilities, and there appeared to be a strong correlation between their job title and Jaques' (1996) suggestion for the types of individuals that fill these roles.

Such individuals are those who consider a situation and work out alternative pathways through which problems can be solved. This level of work requires a strong diagnostic capability, and the ability to consider both short and long term needs and consequences (Jaques, 1996, p. 67).

4.4.3 Assessed As Stratum Four

One respondent (11%) was assessed to be working at Stratum Four. The WMS tool provided a clear grouping of responses assessing this individual at Stratum Four. Interestingly, the respondent has provided a Stratum Two or Three job title, but self-assessed themselves as a Stratum Four worker.

It is considered that Stratum Four individuals are managers who must be capable of pursuing a number of projects simultaneously, with alternatives ready if they should fail. Consequently, work at

this level requires adjusting projects in relation to each other, and ensuring limited resources are managed effectively between them (Jaques, 1996, p. 68).

4.5 Interpretation

In consideration of the analysis, a number of underlying themes emerge. These themes are congruent with the underlying theory posited by Jaques (1976, 1996, 2002), and provide insight to the nature of the stratum of work within the corporate security function. These themes will be discussed in aid of responding to the research questions. Research question one is:

(1) What is the stratum of security managers in the corporate organisation context?

Research question two is;

(2) To what extent does the corporate security function permeate throughout organisations?

As discussed Davis and Moore (1945) and Durkheim (1984), society is a stratified system in which individuals perform a specific role for society. Wilensky (1964) builds on this claim and discusses the continuing specialisation and proffesionalisation of these stratified roles. Consequently, security as a discipline is one such stratified domain that is pursuing professionalisation (Interim Security Professionals Taskforce, 2008). Furthermore, due to the nature of stratification within society, it is assumed that an underlying stratum of security practitioners exist along the broader occupational stratum of work in aid of fulfilling the many roles required within the corporate security function. This assumption of a stratum of security practitioners stems from Fayol's (1949) articulation of the corporate security activity within organisations and Jaques (1996, 2002) framework for examining the stratification within the workforce, which for this study has been applied to the corporate security context.

4.5.1 Types and Levels of Work within the Corporate Security Context

The analysis indicates that the corporate security stratum of work encompasses Stratum Two, Three and Four. These strata are operationally focussed, with Stratum Four shifting focus to longer term issues and providing more support for overall organisational objectives (Jaques, 1996, pp. 65-70). This analysis indicates that the work conducted by the corporate security function is at the lower tiers of an organisation, operating at a tactical and operational strata of work. As dictated by the literature, corporate security is a practice area of management that is focussed on risk reduction through security controls (Brooks & Corkill, 2014; Smith & Brooks, 2012; Fischer et al., 2008; Garcia, 2008; Talbot & Jakeman, 2009). Congruent with this understanding, Jaques (1976, 1996, 2002) explains that Stratum Five is the highest level of work that domain specific tasks and responsibilities are conducted, and as such, logically corporate security should fall at or below this strata.

Whilst it is generally accepted in the literature that corporate security can be used as a strategic function that supports and value adds to organisational objectives (Smith & Brooks, 2012; Fischer et al., 2008; Talbot & Jakeman, 2009), the pilot study analysis does not support this hypothesis. Nevertheless, corporate security does have a contribution to the long term planning and operation of an organisation; which requires engagement with those operating at the executive stratum of

work, or for an individual to champion the security cause at the executive level without necessarily being directly affiliated with the corporate security practice area.

Significantly, the pilot study analysis indicates that corporate security practitioners are confined to a business unit, and do not operate at a level of work conducive to influencing strategic objectives. For this to change, individuals would have to shift from their current identified level of work, and move beyond Stratum Five, as this is where the nature of an individual's work becomes more general and directly supportive of overall business operations; including providing strategic direction (Jaques, 1996). The implications of the pilot study suggest a significant disconnect between the corporate security and socio-organisational literature in this regard. Such a disconnect is to be tested in the main study.

Brooks and Corkill (2014) suggest that within the security business unit, business specific skills become more relevant and salient as seniority increases. Consequently, as these business skills increase in importance, security specific skills are less significant. Mumford, Campion, and Morgeson (2007) agree with this view point, positing that junior and mid-level roles utilise very little strategic skills in their work in comparison to higher level roles. Therefore, the confinement of the security function to its business unit supports these conclusions. Significantly, the analysis indicates that the work conducted within the corporate security domain is relegated to mid-level and junior roles within an organisation, with limited executive engagement on long term issues. This finding is supported by the socio-organisational literature.

4.5.2 Security Decision Making

Talbot and Jakeman (2009), Bayuk, (2010), and Cubbage and Brooks (2013) suggest that security decision making should ultimately be made within the executive levels of an organisation. They argue that a Chief Security Officer should be responsible for all security related issues across an organisation; ensuring the security function is value adding and supporting long term business objectives (Smith & Brooks, 2012). The analysis indicates that this is not the case in practice, and suggests a significant disconnect in the corporate security and socio-organisational literature. Furthermore, as no respondents exceeded Stratum Four, the findings support that corporate security is limited to decision making within a business unit, with little influence on the higher levels of an organisation, again, an assertion to be tested in the main study.

Significantly, as discussed by Brooks and Coole (2011), the corporate security practitioner has not had the opportunity to contribute fully to an organisation. It could be argued from this analysis that the confinement of the corporate security function, alongside a misunderstanding of the capabilities of the corporate security practice area could be responsible for this. Nevertheless, this analysis suggests that security may not yet be considered a strategic function within an organisation, and until it can demonstrate its worth to the overall organisation this perception will not change (McGee, 2006).

4.6 Implication for Main Study

The analysis conducted in Section 4.4 and the discussion in Section 4.5 provides a baseline for the expectations coming out of the main study. This analysis indicates that the methodology is sound, that the survey construction is valid, and that only some minor changes need to be adopted for the

main study's instrument. Consequently, through the analysis, 54% of responses to the TCMT were assessed as Stratum Six and above, where no responses were assessed as above Stratum Five. Significantly, this response indicates a restructure to the instrument is required (Appendix D). Such a restructure included the rewording of the TCMT instrument to use a more common vernacular with appreciation for the range of individuals undertaking the survey, as well as the inclusion of further cross check measures within the WMS and exclusion of certain questions that were deemed to be extraneous for the intended purpose of the study.

4.6.1 Identified Themes

Four primary themes developed out of the analysis and discussion. First, there is evidence of a significant disconnect between the corporate security and socio-organisational literature. Second, the confinement of the security function to within a business unit is prevalent in the analysis. Third, the analysis suggests that the concept of a corporate security champion operating at the executive stratum of work may not be entirely valid. Finally, security decision making is, according to the analysis, heavily restricted in its reach and impact to the higher levels of the organisation.

4.6.2 Limitations of Pilot

The pilot study had a number of limitations which must be addressed when considering the analysis and discussion in Sections 4.4 and 4.5. Firstly, the limited sample size of this pilot study has the potential to skew the analysis and provide false insights into the stratum of work within the corporate security function. Furthermore, in line with this potential skew is the fact that only managerial level responses have been completed in full, providing no analysis of Stratum One workers. Moreover, Boal and Whitehead (1992) suggest that Jaques' underlying theory is not robust enough to be applied to all situations. Significantly, they suggest that cognitive capacity must be considered in conjunction with behavioural traits. Therefore, through consideration of work conducted by Ivanov (2011), it could be argued that Jaques' underlying theory may require further development, especially in terms of the relationship between the complexity of work, and individual's time-span of discretion.

4.7 Conclusion

This chapter presented the pilot study which provided a trial run of the proposed research methodology. This trial established the feasibility of the study, explored the analysis methods to be used, and examined the research instruments for use in the main study. Furthermore, the pilot study used a small sample to examine this feasibility, and results were analysed and discussed in relation to the research questions. Consequently, the pilot study identified that the corporate security stratum of work is between Stratum Two and Four. Significantly, this finding indicates a disconnect between the broader socio-organisational literature and the corporate security body of knowledge. Nevertheless, the pilot study demonstrated the proposed methodology was sound, and that the survey instruments required some minor adjustments to improve their measurement accuracy in the main study.

CHAPTER FIVE: ANALYSIS

Chapter Five presents an analysis of the main study data in relation to the posed research questions. In consideration of a stratified society in which work is conducted through a variety of hierarchical and differentiated occupations, the analysis examined the stratification of corporate security work within the corporate domain. The analysis used Jaques' (1996) occupational stratification framework to examine the levels of work within the corporate practice area of security. This framework guided instrument design and use including the weighting of some measurements over others to provide a more robust and consistent measure of work. Nevertheless, some inconsistency between measures existed, therefore the chapter also discusses the study's reliability and validity (Section 5.4), supported by an examination of the methodology and instrument construction to inform the summary of the analysis' findings.

5.1 Participants

In total, approximately 200 participants were selected to undertake the survey which was distributed through personal and professional networks of the researcher and research supervisors. This distribution was achieved through email, magazine advertisement and social media websites such as LinkedIn. Initially, the research team purposively selected approximately 100 participants across the stratum of corporate security work, who were assumed to have sent at least one email to another participant as requested by the researcher. Out of these 200 individuals a response rate of 21% was achieved. From the 42 responses, there were five non-responses and four un-assessable responses, leaving a response sample of 33 assessable survey questionnaires for analysis.

5.2 Response Data

Data was separated from the completed surveys and tabulated for initial analysis (Appendix E). Individual responses were extracted and listed in the appropriate tabulated columns. These columns were the Work Measurement Scale (WMS), Task Complexity Measurement Tool (TCMT) and Assessed Level of Work results. The Job Level column represents a participant’s selected response of their perceived level of work for validity cross check purposes. Following tabulation, data averages and standard deviations were calculated and listed for further analysis. Consequently the average result column measures the average level of work across the job level, WMS result and TCMT result.

5.2.1 Analysis

Data analysis was conducted; with groupings of responses providing indication of an individual’s level of work (Section 3.3). Incomplete responses are listed in Appendix A as they provide insight into the survey construction. Each response was assessed, with the final assessed level of work score judged based on control questions, overall Task Complexity Measurement Tool (TCMT) and Work Measurement Scale (WMS) results. Furthermore, the final assessed level of work score considered the cross check measures such as job title, self-identified work level, and number of employees managed.

Analysis indicates the stratum of security work within the corporate organisation spans from Stratum One through to Stratum Four. Furthermore, analysis supports that a general job title alignment across each strata exists for the corporate security participant sample. However, the number of employees managed at each strata varies, with the average employee count for Stratum One being three employees, for Stratum Two 12 employees, for Stratum Three 10 employees, and for Stratum Four 65 employees (Appendix E).

Assessed as Stratum One

11 respondents (33%) were assessed to be Stratum One (*Table 5*), through groupings of responses in the WMS. Of these respondents, 36% accurately identified their level of work. However, further examination of each response indicated that 64% of respondents supervised subordinate staff, which is contrary to Jaques (1996) work, indicating potential misalignment of the measure. Furthermore, there was no consistency in job titles across this strata, with only 18% of responses demonstrating a Stratum One work title when aligned to Jaques (1996).

Table 5. Stratum One responses

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work	Average Level of Work	Standard Deviation
Stratum I							
Business Proprietor	3	IV	I	VI	I	3.67	2.05
Security/Comms Technician	1	I	I	IV	I	2.00	1.41
Not Assessed	Not Assessed	I	I	VII	I	4.33	2.83
Sales and Technical Support	0	I	I	IV	I	1.75	1.41
Not Assessed	1	IV	I	V	I	3.33	1.7
Not Assessed	0	I	I	I	I	1.00	0
Assistant Director	10	III	I	IV	I	2.67	1.25
CEO	15	VII	I	VII	I	4.67	2.83
Not Assessed	1	Not Assessed	I	VI	I	3.50	2.5
Not Assessed	Not Assessed	II	I	Not Assessed	I	1.50	0.5
Consultant	3	VII	I	VI	I	4.67	2.62

The mean and standard deviation data in the Stratum One response category indicates that there is extensive variance between the self-identified work level, the WMS result and the TCMT result. These variances indicate inconsistencies between the measurement instruments. Consequently, the TCMT tool proved unreliable in its measurement of work for this strata as there was limited consistency with the WMS result.

In addition, three responses within the Stratum One category at first glance appeared out of place by their identified job title. These three responses, the CEO, Business Proprietor, and Assistant Director would be heuristically considered as much higher strata roles. However, after further examination of their responses to the WMS, each reputed a Stratum One alignment. Such a misalignment is explained by Ivanov's work, which suggests that small business owners and operators tend to misalign with Jaques' framework due to the localised nature of small business operations (2006). Furthermore, Laner et al. (1969), and Allison and Morfitt (1994) acknowledge that accurate

measurement of responsibility at the lower stratum of work can be difficult which may contribute to these findings.

Assessed as Stratum Two

12 respondents (36%) were assessed to be Stratum Two (*Table 6*), with 8% of responses accurately identifying their job level. Furthermore, 25% of these respondents indicated a Stratum Two job title, and 50% revealed that they manage subordinates in their role. All respondents in this category indicated response groupings in the WMS which correlated to a Stratum Two work role. Nevertheless, the TCMT did not indicate consistency with the WMS measure.

Table 6. Stratum Two responses

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work	Average Level of Work	Standard Deviation
Stratum II							
Security Coordinator	50	III	II	VII	II	4.00	2.16
Country Security Manager	20	IV	I	IV	II	3.00	1.41
Associate Security Consultant	3	III	II	IV	II	3.00	0.82
Not assessed	Not Assessed	V	II	IV	II	3.67	1.25
Principal Consultant – Security & Risk	0	I	II	VI	II	3.00	2.16
Senior Consultant, Crisis & Security Consulting, Middle East	0	Not Assessed	II	V	II	3.50	1.5
Not Assessed	Not Assessed	II	II	V	II	3.00	1.41
Not Assessed	6	III	I	IV	II	2.67	1.25
Not Assessed	4	IV	II	VI	II	4.00	1.63
Security Coordinator	0	III	II	IV	II	3.00	0.82
Not Assessed	Not Assessed	I	II	VI	II	3.00	2.16
Not Assessed	60	III	II	VII	II	4.00	2.16

The average level of work within this category exceeded the assessed response, with a mean standard deviation of 1.56. This standard deviation indicates the need to weight the more consistent WMS score as more significant than the less consistent TCMT score in the analysis.

Assessed as Stratum Three

Seven respondents (21%) were assessed to be Stratum Three (

Table 7), with 57% of respondents accurately identifying their own level of work. Nevertheless, job titles in this category varied, however they indicate a consistency for the identified strata of work (Jaques, 1996). For example, 57% of responses indicated a Stratum Three job title, with 43% identifying that they manage subordinates in their role. Consequently the TCMT tool again indicated some consistency across responses, but no correlation to the WMS.

Table 7. Stratum Three responses

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work	Average Level of Work	Standard Deviation
Stratum III							
Lead Security Consultant	0	III	III	II	III	2.67	0.47
Security Program Manager	0	III	III	IV	III	3.33	0.47
Security Manager	8	III	III	IV	III	3.33	0.47
Security Professional	0	I	III	VI	III	3.33	2.05
Not Assessed	30	III	II	IV	III	3.00	0.82
Not Assessed	30	IV	III	VII	III	4.67	1.7
Director – Adjunct Ass Prof	0	VII	III	IV	III	4.67	1.7

Jaques (1996) work indicated that Stratum Three individuals are those who consider a situation and identify alternative pathways through which problems can be solved. This level of work requires a strong diagnostic capability, and the ability to consider both short and long term needs and consequences (Jaques, 1996, p. 67). The average work level for this strata was consistent with this body of work, and was more indicative of the final assessment (Appendix A). This assessment is supported by the standard deviation (1.09) which indicated less variance across measurement tools than in the lower strata measures. In this case, a lower standard deviation across the measurement tools provides insight into the consistency of responses in relation to the identified level of work. According to Laner et al. (1969) and Allison and Morfitt (1994) this is indicative of Jaques' measurement of responsibility being more effectual for higher levels of work.

Assessed As Stratum Four

Three respondents (9%) were assessed to be Stratum Four (*Table 8*), with one respondent underestimating and two respondents overestimating their job level. Consequently, 33% of responses identified a job title that was inconsistent with the level of work identified. However, those participants assessed as meeting the criteria for Stratum Four indicated a strong correlation in terms of number of employees managed to Jaques strata of work, with 100% of respondents at this level identifying they manage subordinates, and 67% managing more than 50 subordinates.

Table 8. Stratum Four responses

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work	Average Level of Work	Standard Deviation
Stratum IV							
Not Assessed	5	III	IV	V	IV	4.00	0.82
Not Assessed	100	VII	IV	VII	IV	6.00	1.41
National Security Director	90	V	IV	VI	IV	5.00	0.82

The average work measure at this strata varied between stratums four through to six, with a mean standard deviation of 1.02. This standard deviation indicates a strong correlation across data

components, demonstrating a low variance between data collection tools. A smaller variance across each tool provides a more reliable measurement of the individual's level of work. Individuals at this level were subject to the same weighting towards the WMS result as the lower level strata responses to ensure consistency.

5.2.2 Data Considerations

An analysis of occupational work strata (*Figure 7*) indicates the majority of participants work within the first two strata of work (70%), with work levels reducing across Stratum Three and four (30%) for the participant sample.

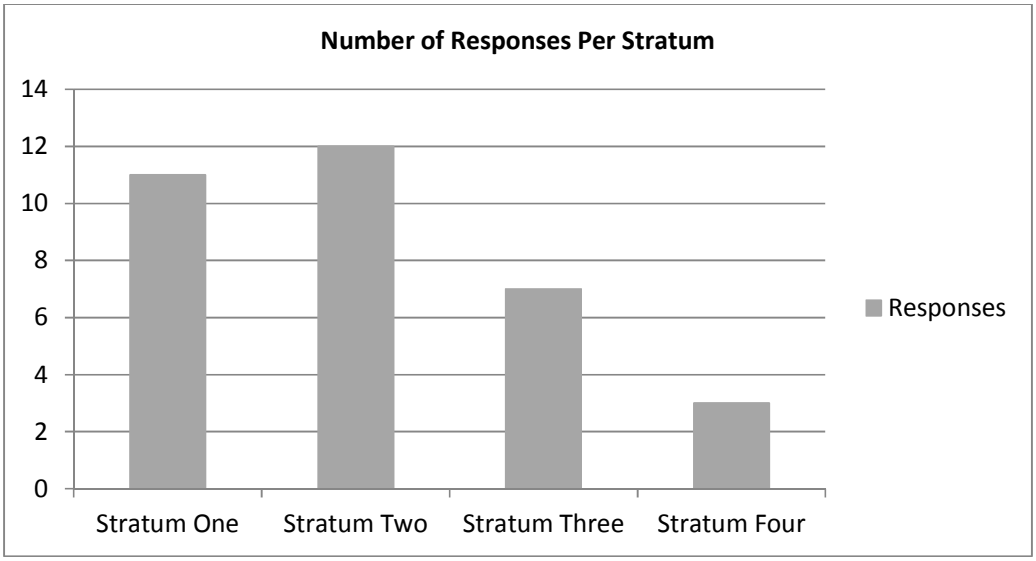

Figure 7. Number of responses per stratum of work

An analysis of the data indicates that security practitioners operating in the first two strata of work demonstrated a low level (22%) of job title alignment to their level of work, and that Stratum Three and Four operatives demonstrated a moderate job title alignment of 50%. This indicates a more defined role understanding at the higher strata of work within the corporate security domain.

5.3 Data Analysis Reliability and Validity

Analysis was conducted with the consideration of the instrument construction, alongside the reliability and validity of the study. The methodology (Chapter 3) highlighted some potential limitations with the survey design which were addressed, however consideration will be given to the pilot study (Chapter 4) and main study to aid in this analysis.

Through a comparison of each individual response, a plot of the assessed level of work in relation to the mean level of work was conducted. Consequently, a review of the instruments reliability and validity can be conducted. The mean level of work was acquired over the self-identified work level, the Work Measurement Scale (WMS) score and the Task Complexity Measurement Tool (TCMT) score (Equation 2).

Equation 2: $$Mean\ Level\ of\ Work = \frac{Self\ Measure + WMS\ Measure + TCMT\ Measure}{3}$$

Consideration of this mean level of work score and the standard deviation of the score in relation to the assessed level of work score can provide insight into the reliability of the measurement instruments. *Figure 8* demonstrates this as an example, with four varying scores presented and the assessed reliability of the data.

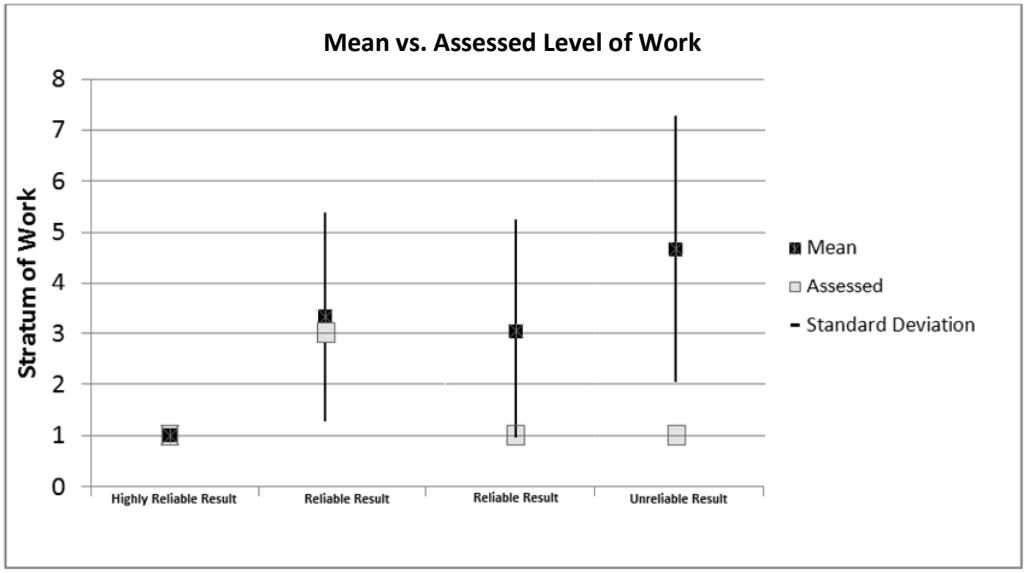

Figure 8. Mean vs. Assessed Level of Work Example

Figure 9 provides a plotted SD as an indicator of reliability across research instruments. The majority of assessed responses (72%) correspond to the identified standard deviation, indicating the assessed level of work has fallen within the variance between measurement instruments. This outcome is significant as it identifies that the weighting of the WMS score over the TCMT score was a reliable measure of work. Furthermore, it indicates validity in the data and assessment method as the majority of responses have been assessed within the variance of each work measure.

Stratum One respondents were the most difficult to align within Jaques' (1996) stratum of work; with scores indicating minimal adherence to the mean or standard deviation between assessable outcomes. However, in consideration of the results discussed by Laner, Crossman, and Baker (1969) and Allison and Morfitt (1994) such an outcome is not surprising. Stratum One rankings have little correlation with the mean level of work score, with 90% of the mean level of work scores falling outside of the assessed level of work score. Furthermore, 45% of scores at Stratum One fell within their standard deviation away from the assessed score. This analysis indicates that the measurement of work at Stratum One may be unreliable.

Stratum Two scores (*Figure 9*) have a strong correlation with the mean level of work score. Whilst 100% of mean level of work scores fell outside of the assessed level of work score, 83% of these scores fell within their standard deviation from the assessed score. In consideration of this analysis, it is likely that the Stratum Two measurements are reliable.

At Stratum Three, 14% of the mean level of work scores aligned with the assessed level of work score. However, 100% of scores fell within the standard deviation from the mean. Significantly, this indicates a strong correlation and reliability in the measurement instruments for this level of work.

Stratum Four scores were less reliable than Stratum Three, with 33% of the mean level of work scores aligning with the assessed level of work score, and 66% of scores falling within the standard deviation. Consequently, Stratum Two and Three scores are the most reliable, followed by Stratum Four and finally Stratum One.

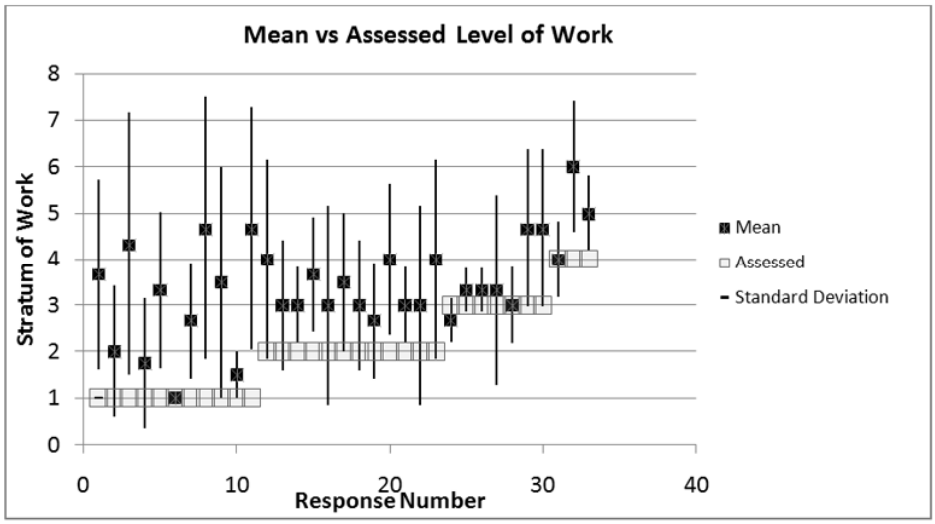

Figure 9. Mean vs. Assessed Level of Work

Findings indicate a relationship between the mean value identified through the self-assessed level of work, the WMS result and the TCMT result when compared to the analysed levels of work assessment (*Figure 10*). This comparison indicates the validity of the analysis, enabling a weighting towards the WMS result. The standard deviation trend line decreases as the strata of work increases, mirroring expectations put forward by Laner, Crossman, and Baker (1969) and Allison and Morfitt (1994) who suggest that the measurement of work put forward by Jaques' can be difficult to apply to lower levels of the occupational stratum.

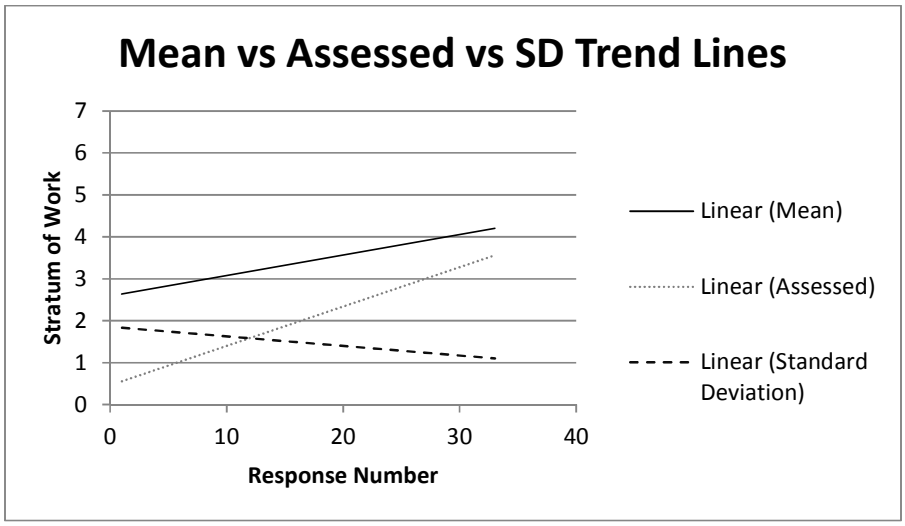

Figure 10. Mean vs. Assessed Level of Work vs. Standard Deviation Trends

5.3.2 Instrument

The instrument, comprised of two tools, underwent an iterative design process over the course of the research. Initially the tools were developed accordant with the literature, and then submitted for review to the research supervisors, who provided insight and feedback. This feedback was considered, with relevant changes made and an updated variant of the instrument then distributed for discussion. Consequently, the instrument was tested via a Pilot Study (Chapter 4), where analysis was undertaken, and then final revisions conducted before administration in the main study (Colton and Covert, 2007, p. 18)**.**

Work Measurement Scale

The Work Measurement Scale (WMS) was developed to measure the task-time span of an individual within their work role. This tool was developed by the researcher through analysis of the literature, drawing from work conducted by Jaques (1964, 1972, 1996) and Mintzberg (1973, 1980). Jaques (1964) identified that the measurement of an individual's task time span can only be achieved through direct discussion with the individuals' manager, and that manager's manager. Due to the study design, time restrictions of the project and the limitations of online surveys, this could not be achieved, leading to the development of the WMS tool built on the work of Mintzberg. Mintzberg (1973) articulated the various aspects of a manager's work, and detailed the differences between lower strata workers and higher strata workers. Utilising these insights, the WMS was designed to measure multiple aspects of an individual's work in aid of identifying the longest task time span.

Reliability is the extent that an instrument produces the same information across multiple uses (Colton & Covert, 2007, pp. 73-75). The WMS was used in the pilot study and the main study, providing similar results across the two samples. Such consistency indicates reliability in the tools design. In addition, internal consistency can be measured through a comparison of results across items within an instrument through a single sample (Colton & Covert, 2007, pp. 73-75). Consequently, the WMS indicated internal consistency in both the pilot study and the main study through provision of measureable and consistent results.

Validity is a demonstration of an instruments ability to measure what it purports to measure (Colton & Covert, 2007, pp. 65-73). Significantly, the WMS has achieved validity through a number of forms. Firstly, the tool meets requirements for content validity, as it is representative of the literature and the process being investigated by the research (Cohen, Manion, & Morrison, 2007; Colton & Covert, 2007). Secondly, construct validity has also been indicated in this tool, as it has met requirements for convergent validity; where an instrument can show a relationship between constructs that should have a relationship with each other (Colton & Covert, 2007). Convergent validity was indicated by this tool through multiple aspects of an individual's work as outlined by Mintzberg (1973) aligning along the time-span of discretion measurement in the instrument. Conferring with the work of Cohen, et al., (2007) face validity was determined by two security academics supervising the research project.

Task Complexity Measurement Tool

The Task Complexity Measurement Tool (TCMT) was adapted from a scale used by Jaques (1996, p. 72) in the measurement of task complexity inherently found in a particular project or role. The TCMT was designed to provide a cross check measure for the individuals self-identified level of work in the WMS. The TCMT, rather than measuring the task time of an individual, instead measured the task complexity experienced by an individual. According to Jaques (1964, 1970, 1972, 1976, 1996), these two phenomenon are inextricably linked in identifying an individual's stratum of work.

Whilst this tool was adapted directly from the literature, and thus can be argued to have already met face validity requirements for its use, it is important to note the tools limitations throughout both the pilot study and the main study (Christensen & Johnson, 2014; Cohen et al., 2007; Colton & Covert, 2007). Further consideration must also be given to the tools design and purpose, and perhaps its limitations as an online survey. Jaques (1996, p. 72) acknowledged the measurement of task complexity to be subjective and descriptive, and therefore stated that this must be measured in liaison with the individuals manager and the managers' manager. This qualitative approach was not possible for the online survey, and without the individuals' superiors oversight, it is possible that the tool did not uncover individual's exact levels of work. It is further suggested that consideration be given to the age of the tool, and the significant changes that have occurred in the workforce in terms of task complexity; especially in terms of modern technology and information throughput. These factors may have contributed to the tools inability to provide a concrete cross check measure for the WMS.

5.4 Conclusion

This chapter presented the analysis of the main study, with 33 usable responses. Response data was tabulated and analysis conducted, with data broken down into work strata. This category alignment between Stratum One to Stratum Four was further discussed for understanding. Responses in each strata were assessed on a variety of factors, and consideration was given to cross check measures inbuilt into the research instrument. The research instrument was considered in terms of reliability and validity, with the Work Management Scale (WMS) demonstrating both reliability and validity throughout the study. However, while the Task Complexity Measurement Tool (TCMT) was adapted from the literature, it did not provide a strong correlation with the WMS. This lead to the researcher weighting the WMS response as more significant than TCMT response in the analysis. Nevertheless,

the analysed data allowed interpretation of the data to respond to the Research Questions, which will be discussion in the next chapter.

CHAPTER SIX: INTERPRETATION AND DISCUSSION

Chapter Six presents the interpretation of the study in response to the posed research questions. The chapter reintroduces the literature and research questions (Section) along with the supporting analysis. Significantly, the research questions are responded to in consideration of corporate security as a practice area within the occupational stratum of work in society. Therefore, the discussion considers corporate security within the context of the management domain and provides analysis based on Jaques theoretical works (1996). Furthermore, findings collected from the analysis will be discussed in detail, including pertinent insights that do not directly relate to the research questions (Section 6.2).

6.1 Understanding the Corporate Security Stratum of Work

The study investigated the stratum of work in the corporate security domain to respond to questions posed in relation to its functional position within the broader occupational strata of work in organisations. In consideration of a differentiated and stratified society, as postulated by Durkheim (1984) and Parsons (1951), the practicing domain of corporate security acts as a specialised and functionally important (Davis & Moore, 1945) occupation that is deeply embedded in the operation of organisations (Fayol, 1949). Corporate security, as with other occupational domains, is tied to the notion of ever increasing work specialisation through rising complexity within society. This specialisation is evidenced by the growth currently being experienced by the security industry at large (Prenzler et al., 2009) due to the inherent complexity associated with globalisation in modern society (Stichweh, 2008). The corporate security stratum of work was explored through the Research Questions: (1) *What is the stratum of security practitioners in the corporate context?* and (2) *To what extent does the corporate security function permeate throughout organisations?*

6.1.2 Research Question One

In response to the question: *what is the stratum of security practitioners in the corporate context?* The study identified that four distinct strata of work exist within the corporate security function. That is, the strum commences at Stratum One and includes Stratums Two, Three and Four, with no participants working beyond Stratum Four. Consequently, corporate security is predominately a lower strata occupational undertaking with the majority of participants indicating that they operate at Stratum Two. Such a finding has significant implications for the corporate security literature as it uncovers a significant disconnect between the corporate security and socio-organisational literature.

In contrast to the findings of this study, the corporate security literature perceives the function to be a strategic activity within an organisation, ideally operating at the executive stratum of work (Bayuk, 2010; Sennewald, 2011; Brooks and Corkill, 2014). This view is disputed by the findings of the study, which are supported by the broader socio-organisational literature. Significantly, the study findings indicate that in contrast to the published corporate security literature, security is a lower strata function within organisations, and at best is a middle level strata occupation with no strategic decision making or influence at the executive level. Furthermore, the study revealed four distinct strata of work, which provides clarification of the levels of work in the corporate security function;

aligning the corporate security literature to the socio-organisational perspective of business activities.

The study uncovered that the weighting of security works is between Stratum One and Two, with no evidence of practitioners beyond Stratum Four. Nevertheless, the literature suggests that these lower work levels require strong technical and specialist skills that allow for work to be conducted within niche areas. Jaques' (1996) research articulated that work conducted between these levels of an organisation is confined within a business unit, and is thus tactically and operationally focussed. Furthermore, the literature articulates that as a person progresses up the stratum of work, technical skills fall off, and general managerial skills increase in importance (Jaques, 1996). Therefore, corporate security should be considered along this progression (*Figure 11*).

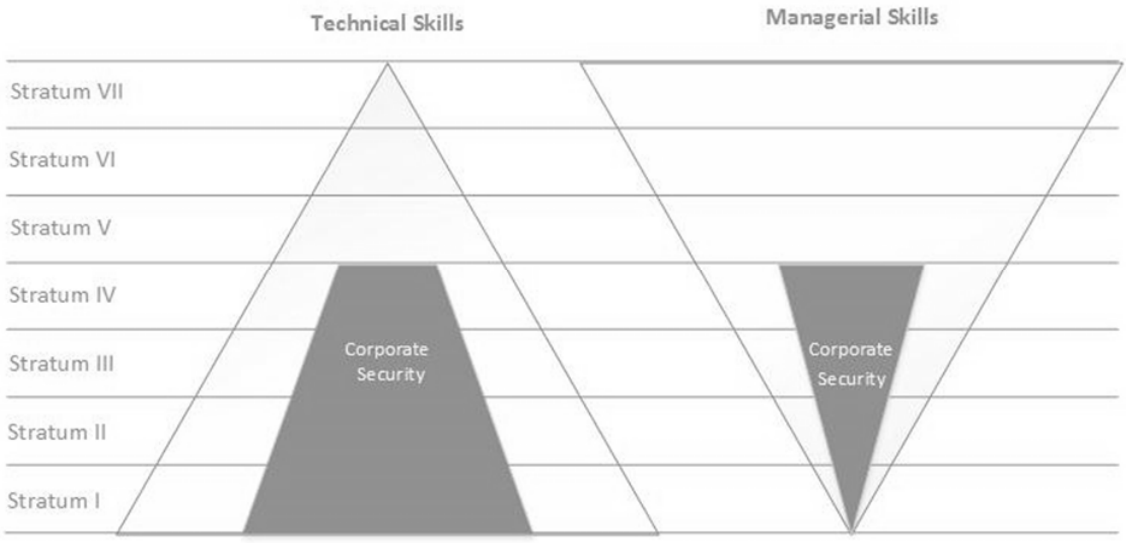

Figure 11. Corporate security skills along the stratum of work

This skill progression (*Figure 11*) provides a starting point for considering each level of identified work in more detail. The four distinct strata of work identified by the findings indicate that the majority of work is conducted by corporate security personnel within an operational time horizon of one day to one year. Analysis correlates this operational level of work with Stratum One and Stratum Two roles; comprising of direct and visible problems, and restricted and highly specialist work environments (Mintzberg 1973; Jaques, 1996). Consequently, tactical time horizons are encountered at Stratum Three and Stratum Four, between a functional time horizon of one and five years. These levels of work involve progressively more abstract thinking, stakeholder engagement and managerial skills. Significantly, the strata identified comprise the lower half of the broader occupational stratum of work in organisations, indicating corporate security's functional boundaries as a subset of this whole (*Table 9*).

Table 9. Identified corporate security stratum of work

Stratum	Role Title	Function Descriptor	Role Type
One	Security Guard, Security Technician, Investigator,	Work is service oriented, and focussed on operational tasks that can be overcome or mitigated through direct trial and error approaches to security control, and	**Operational** One Day - One

	Security Consultant, Sales and Technical Support, Locksmith	problems can be solved with technical knowledge and pre-learned behaviours and tools.	Year
Two	Security Supervisor, Senior Security Consultant, Security Coordinator	Work is restricted to specific operational boundaries and involves problem solving that cannot be wholly tackled by pre-learned behaviour. Individuals must collect information about a problem using security knowledge and skills to provide a solution to an immediate security objective.	
Three	Security Manager (Specialist) / Lead Security Consultant	Work requires strong diagnostic skills to solve security problems. Individuals must consider a situation using their technical security knowledge, and some generic managerial skills in their interaction with internal and external stakeholders to develop short term mitigation strategies whilst considering consequences.	**Tactical** One Year - Five Years
Four	Security Director / National Security Director	Work becomes unstructured and ill-defined, with multiple projects occurring simultaneously. Individuals move away from strong technical security knowledge and begin to harness generic managerial skills in the management of budgets, staff, and projects to meet medium term risk mitigation strategies.	
Five	NA	NA	
Six	NA	NA	**Strategic** Five Years - 20+ Years
Seven	NA	NA	

Stratum 1: Front Line Workers

When aligned with the work of Jaques (1996), corporate security practitioners operating at Stratum One of work are responsible for operational actions and problem solving within an organisation (Jaques, 1996). The socio-organisational literature articulates that practitioners operating within this level have a reliance on training and organisational procedures to delineate and bound their work operations and tasks (Martin & Fellenz, 2010). Consequently, practitioners operating at this strata of work solve problems through direct actions (Jaques, 1996), and are the face of the corporate security function to the broader organisation (Sennewald, 2011). Jaques' articulates that Stratum One workers require supervisor oversight and direction when faced with a problem that cannot be tackled by procedures and training (1996). Therefore, it is further articulated by the literature that roles at this level have a strong technical and procedural focus with no managerial skills required in work. The findings indicate that there is alignment between the corporate security and socio-organisational literature at this stratum of work, lending validity to the identified work bounds.

Stratum 2: Front Line Manager

Findings indicate that there is a significant disconnect in the literature at the Stratum Two level of work. The socio-organisational literature articulates the functions of a front line manager (Jaques, 1996), however the security literature has limited alignment to this articulation and limited consensus amongst its own body of work. Barefoot and Maxwell (1987) in discussion of role descriptions within corporate security do not articulate a Stratum Two role, jumping from front-line workers up to middle management. Furthermore, Fay's (2002) discourse on the corporate security

function does not detail the roles or responsibilities of any stratum of work, instead opting for generic descriptions of function outputs. Significantly, the Interim Security Professional's Taskforce (2008) articulate three roles with significant overlap in responsibilities from a generic managerial perspective, namely the security staff, shift leader and the supervisor. The shift leader in particular borrows elements from the Stratum One worker and Stratum Two worker, with responsibilities that would be better aligned to the front line or supervisory role. It can be argued from the perspective of the management literature that this role articulation is misinformed and misaligned within the organisational context, leading to conflicting and inefficient staffing (Ivanov, 2011).

Furthermore, Sennewald (2011) in his discourse on the stratum of the corporate security function identifies the role of a security supervisor. This is supported by the Interim Security Professional's Taskforce (2008) who articulate the role to include the direction, training, discipline, and oversight of front line workers. Whilst inconsistencies arise in the seating of the supervisor role between these authors, their prescribed work outputs are in fact consistent. Brooks and Corkill (2014) further discuss the front line managerial role within the corporate security function with alignment to the discussion postulated by Sennewald (2011). However, this discussion goes too far and attributes Stratum Three responsibilities such as applying higher level policy in their work, and liaising with external stakeholders in the provision of staff and other vital services.

Jaques (1996) articulates that the Stratum Two practitioner is one who has an operational focus with identifiable boundaries of work. Brooks and Corkill (2014) discuss this boundary for a corporate security practitioner as being within one facility or site of operation. Sennewald (2011) articulates a similar boundary of work at this strata. Consequently, it is considered that alongside this clear boundary of work, Stratum Two workers should operate autonomously, bounded by policy and procedures (Jaques, 1996). Jaques postulates that work at this level requires practitioners to problem solve by collecting information before making a decision (1996). In consideration of this role articulation, which can be validated through the socio-organisational literature and supported by the findings, there is strong indication of a significant disconnect between the security and organisational literature at this stratum of work.

Significantly, as the findings indicate that the majority of security work is undertaken at Stratum Two, and with such a conflicting discourse in the security literature for this level of work, it is argued that the literature lacks a clear perception of the actual outputs and functional significance of the corporate security activity area. Furthermore, it is argued that the corporate security literature does not appreciate these conflicting views with each perspective struggling to find an objective viewpoint through which the domain can be examined holistically. Thus many siloed viewpoints are presented in the discussion with no perspective attempting to unify these mismatched and poorly articulated understandings.

Stratum 3: Unit Manager

Jaques (1996) defines Stratum Three roles as those being responsible for the development of new systems and procedures, which prescribe work at the lower strata of operation. The corporate security literature does not distinctly articulate this role as a separate entity within the security function, and instead combines aspects of the Stratum Three role with lower tier security supervisor positions, and higher tier security manager positions (Brooks & Corkill, 2014; Cubbage & Brooks,

2013; Sennewald, 2011). This misalignment of responsibilities is significant as it can result in reduced productivity, excessive red tape, and organisational breakdown in communication (Ivanov, 2011).

Consequently, the findings are supported by the socio-organisational literature and identify the existence of a Stratum Three role within the corporate security function; whose role requires a shift toward undefined managerial tasks (Mintzberg, 1973). Nevertheless, the role still requires technical and specialist knowledge of security in the conduct of work, but this knowledge is leveraged through managerial skills to achieve business objectives (Jaques, 1996). Furthermore, the management literature suggests that a Stratum Three role requires a strong diagnostic ability which is harnessed through an understanding of broader business needs and objectives (Jaques, 1996; Martin & Fellenz, 2010).

According to Jaques, Stratum Three roles focus on internal problems but demonstrate an appreciation for external stakeholders in their work (1996). Significantly, findings indicate that this role may be a specialist security manager or lead security consultant. Such findings again support the proposition indicating that there is a significant disconnect between the security and management literature. This disconnect in the literature is significant as it indicates a systemic misunderstanding of the security function within the broader organisational context.

Stratum 4: General Manager

The study found evidence of Stratum Four work within the corporate security domain. Stratum Four roles require strong managerial skills and the ability to operate as a generalist within a specialist domain (Jaques, 1996). Brooks and Corkill (2014) articulate this role within the corporate security function as being responsible for overseeing lower strata work outputs; ensuring the function is aligning to strategic organisational objectives. Significantly, this discourse correlates with Jaques' discussion of Stratum Four roles being unable to influence strategic direction, but being capable of influencing the way these strategic goals are achieved at a tactical level (1996). Consequently, the literature defines this role within the security context as being a mid-level manager who operates as the interface between the executive level functions and the lower level security functions (Fay, 2002; Sennewald, 2011). While the security literature dictates that roles beyond this level of work exist extending into the executive stratum in corporate security (Bayuk, 2010; Cubbage & Brooks, 2013; Sennewald, 2011), findings indicate that this literature consensus is incorrect. Significantly, study findings support that the Stratum Four corporate security practitioner is the peak of the security function in organisations.

Contextualising the Corporate Security Stratum of Work

The identified stratum of corporate security work within organisations is identified to span the highly specialised and technical operational roles found from Stratum One through to Stratum Four. Jaques (1996) articulates that these work levels within an organisation generally consist of professional roles such as doctors, lawyers, accountants, and engineers; indicating that educational background plays some, but not a significant role in an individual's placement along this stratum of work. Subsequently, Jaques argues that highly specialist educations such as engineering, law, and medicine operate as an accepted pathway and norm to enter such specialist and professional roles in society, but do not guarantee an individual's capacity to progress hierarchically within broader organisational work.

Significantly, this articulation aligns with the nature of the corporate security function, and the identified stratum of work (Fayol, 1949; Smith & Brooks, 2012). Inherently, the application of corporate security within organisations is highly specialised, and is generally populated by individuals with specialist educational backgrounds, or in less professional roles, embedded organisational knowledge that has been passed down through worker transition (Sennewald, 2011). Such specialisation intrinsically restricts individuals to the lower bounds of the organisation, as hierarchical progression is not linked to the application of such knowledge. Consequently, corporate security may be limited in its strategic reach, but this is not an indictment of the individuals who fulfil these roles; such individuals are actually highly capable and knowledgeable about their craft.

On reflection of such findings it is interpreted that those individuals who wish to progress beyond corporate security and enter the executive stratum must be mindful of the inherently different work context (Mintzberg, 1973, Martin & Fellenz, 2010. Subsequently, those exercising strategic governance and direction roles act with a strong generalist skill set, with education and work methods that suit the leveraging of specialist functions to achieve broader organisational goals. Thus, in the pursuit of executive level placement, individuals must shed their specialist affiliation and embrace general organisational practice.

6.1.2 Research Question Two

Research question two asked: *to what extent does the corporate security function permeate throughout organisations?* The study revealed that the corporate security function operates within an organisation as a function of the technostructure; providing analytical advice on business operations. Corporate security leverages its diagnostic, inference, and treatment capabilities to consider tactical and operational problems within the security context; providing advice to the executive and strategic levels of an organisation (Coole, Brooks, & Treagust, 2015). While it is acknowledged that security should be considered at the executive level of an organisation, the socio-organisational literature suggests that this should not be done by a security specialist, directly contesting a consensus in the corporate security literature.

Positioning the Security Function in Organisations

The security literature expounds the view that the corporate security function is a business enabler that can support and strengthen business operations (Sennewald, 2011; Talbot & Jakeman, 2009). Nevertheless, there is a consensus that the function can be considered a cost centre, with no direct impact on increasing market share or profits (Smith & Brooks, 2012; Fischer et al., 2008). In consideration of these points, the security literature argues that the corporate security function should ideally operate strategically within an organisation to ensure it can have greater reach and impact on organisational planning and direction (Cubbage & Brooks, 2013; Fay, 2002; Sennewald, 2011). Furthermore, the literature purports its current relegation to the lower stratum of work is due to immaturity in the industry, lack of a professional consensus, and misunderstandings of the function at higher levels of work in the organisation (Barefoot & Maxwell, 1987; Brooks & Corkill, 2014; McGee, 2006). However, corporate security's roles and positioning can be better clarified through Mintzberg's work (1980).

Mintzberg (1980) outlines three components inherent in any organisational structure, those being the operating core, support staff, and technostructure. The operating core includes staff and

activities that directly correlate to increased profits and the turnover of business. Consequently, it is considered that this operating core is improved through the continued provision of services and innovation of organisational outputs by the executive strata of work (Martin & Fellenz, 2010; Robbins & Judge, 2012). In contrast, findings from the study indicate that consistent with both Jaques' and Mintzberg's work security operates at the lower levels of an organisation, fulfilling a tactical and operational role within supporting functions of an organisation located within the technostructure or support staff. By the nature of these roles, it is argued that security does not operate at the executive level of an organisation.

Security and the Technostructure

The specialist role fulfilled by security practitioners was identified by Fayol (1949) as a core activity of organisational work. However, Mintzberg (1980) and Galbraith (1985) articulated the concept of a technostructure within organisations that consists of disciplines that use specialist analytical problem solving to shape an organisations' exposure to the external operating environment. Significantly, the security literature identifies the function of corporate security to be 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 (Smith & Brooks, 2012; Fischer et al., 2008; Talbot & Jakeman, 2009). Furthermore Coole et al. (2015) articulates that security practitioners utilise an analytical problem solving mindset that requires diagnosis of the problem, inference to develop a protective strategy, and treatment for a solution. Therefore consistent with this body of work it can be argued that corporate security is a function embedded with the technostructure of organisations (*Figure 12* with reference to *Figure 1*). This finding is supported by the broader socio-organisational literature, as it is articulated that technostructure activities provide functions that align with core security objectives (Fayol, 1949; Jaques, 1996; Mintzberg, 1980).

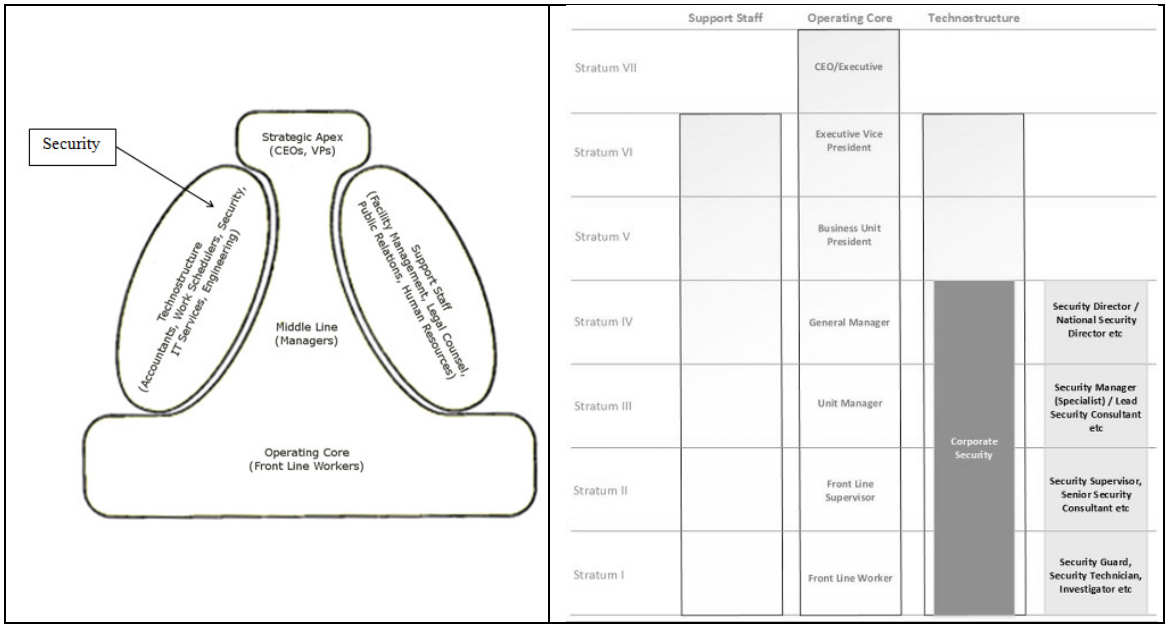

Figure 12. Corporate Security Positioning in the Corporate Organisation, Adjusted from Mintzberg (1980) and Jaques (1996)

Security Decision Making

Brooks and Smith's (2012) discourse on the security champion centres on an individual operating within the corporate security function who is capable of bringing the security perspective to the executive management team; ensuring consideration is given to security issues. Unsurprisingly, the security literature expounds this view, and argues that this individual should operate at the executive level, preferably within the organisational executive team itself (Bayuk, 2010; Brooks & Corkill, 2014; Cubbage & Brooks, 2013; Sennewald, 2011). Significantly, the findings of this study indicate that this literature consensus is not wholly valid; as the alignment of the security function to the tactical and operational levels of work, within the technostructure, do not allow for the security champion to be an insider to the security function and simultaneously operate at the executive stratum of work.

An analysis of the literature supports that the executive level operators within organisations are management generalists with no specialist focus (Fayol, 1949; J. Martin & Fellenz, 2010; Mintzberg, 1973). With this consideration in mind, it is argued that the concept of the security champion is not entirely invalid; however, the individual would not be a security specialist that is embedded within the corporate security function, but rather a senior executive who understands the role of security in achieving business objectives. The security champion, as outlined by the security literature, would be a management generalist who identifies the significance of the corporate security function and leverages the outputs of this function to align with broader organisational strategic objectives. Therefore, this alignment of the security literature to the organisational literature is supported by the findings, and is reinforced by Fayol (1949) who originally outlined this process in his discourse on the corporate security function within organisations.

6.2 Further Interpretations

The analysis has provided insight into other areas that are not directly relevant to the research question, but raise some important points for consideration.

6.2.1 Executive Understanding of Security Function

Jaques' (1996) articulates the importance of identifying the appropriate level of work for individuals within an organisation, especially when delineating responsibilities and types of work. It is vital that managerial hierarchies are established in such a way that each functional level of work can operate at maximum efficiency and with clear communication lines and responsibilities (Ivanov, 2006, 2011). Sennewald's (2011) discourse on corporate security roles outlines the confusion and misalignment of many security practitioners' roles in the industry. Sennewald states that there tends to be an overuse of positional terms in the corporate security domain, with many individuals being wrongly classified as 'security managers' and 'security directors'. This overuse of positional terms leads to role ambiguity and lack of consistency in the domain.

It could be argued that this role misalignment within the corporate security domain is due in part to misunderstanding of the function from the executive team. Jaques (1996) posits that efficient organisational structure requires the executive team to understand individual work capacity in the assignment of responsibilities and roles. Consequently, this understanding of work capacity leads to structured and sensible hierarchies of work as seen in other disciplines such as the medical

profession and the engineering profession (Ivanov, 2011). Significantly, the findings indicate limited job title alignment with each stratum of work, alongside inconsistency in the numbers of staff managed at each stratum of work. Therefore, it could be suggested that this evidence is symptomatic of a misaligned and misunderstood function within organisations that needs rectifying to ensure efficient operation.

6.2.2 Career Pathways

Coole and Brooks (2015) articulate the importance of recruiting and formalising security graduate intakes into organisations to allow for further professionalisation of the industry. However, without understanding of the corporate security disciplines structure, it can be difficult to chart progression within the function. The analysis conducted in this study provides a starting point for mapping career progression, and articulating career pathways within the corporate security function. Individuals begin at the operational level of work, and move towards a more generalist and tactical outlook as they move vertically within the function.

6.3 Conclusion

The chapter discussed the interpretation of the findings in response to the research questions. The study established that there is a significant disconnect between the corporate security and socio-organisational literature. This disconnect is rooted in a misperception of the importance and positioning of the corporate security function by the corporate security literature. The use of the socio-organisational literature has facilitated an objective investigation of the corporate security stratum of work from the context of the broader occupational stratum of work. Through this investigation it is indicated that corporate security operates from the technostructure of an organisation, providing analytical advice to protect organisational interests. Study findings also provided insight into the understanding of the corporate security function from the executive perspective, and developed an understanding of career pathways and progression issues. Consequently consideration must be given to the implications of the results and their significance to the corporate security domain.

CHAPTER SEVEN: RECOMMENDATIONS AND CONCLUSION

The study investigated the stratum of work within the corporate security occupational domain. Significantly, the findings of the study have uncovered a significant disconnect between the corporate security literature, practitioner's perceptions and the socio-organisational literature. Furthermore, the study's findings have also identified the positioning and stratum of work of the corporate security function within organisations. Consequently, this chapter will provide an overview of the study findings and the implications of these findings.

7.1 Study Findings

The study revealed significant findings in response to the research questions. In response to the question: *what is the stratum of security practitioners in the corporate context?* The study uncovered a significant disconnect between the corporate security literature and the broader socio-organisational literature. Consequently, findings suggest that the perception of security as a strategic decision making function with executive reach is not valid. Fayol (1949) originally articulated corporate security as a core business activity, which should be governed by the executive reaches of an organisation; whereas the corporate security literature dictates an executive level function. Significantly, the findings of this study correlate to the broader socio-organisational literature, and position corporate security as a technostructure function not directly aligned to profit generation operations, but still governed by the executive reaches.

Furthermore, the study revealed that the corporate security function operates at the tactical and operational levels between Stratum One and Stratum Four. This level of operation indicates that corporate security practitioners operate within a maximum of a five year time horizon. Of the research sample, 33% of participants were found to be working at Stratum One work in the corporate security function. Such work very direct and restricted in scope, with practitioners relying on procedures and training to solve problems. 36% of participants were found to be working at Stratum Two, such work is broader in scope but restricted to specific operational boundaries, with capacity to draw on basic problem solving skills to solve immediate problems. 21% of participants were found to be working at Stratum Three, where workers require a strong diagnostic ability which can be applied in conjunction with extensive internal and some external stakeholder liaison. Finally, 9% of participants were found to be working at Stratum Four work which includes unstructured and ill-defined tasks, with practitioners being responsible for managing multiple projects simultaneously. Consequently, these findings articulate the roles, their hierarchical seating, and occupational scope within the corporate security function, establishing boundaries of work and providing insight into the reach of the organisational function.

In response to the question: *to what extent does the corporate security function permeate throughout organisations?* The study established that the corporate security function operates within an organisation as a function of the technostructure; providing specialised services and analytical advice to enhance business operations. Significantly, corporate security leverages its diagnostic, inference, and treatment capabilities to consider tactical and operational problems within the security context; providing advice to the executive and strategic levels of an organisation (Coole et al., 2015) on managing the risks associated with a malevolent human adversary. Whilst it is

agreed that security concerns should be considered at the executive level of an organisation; the socio-organisational literature outlines that this should not be done by a highly technical security specialist. Consequently, there is a significant disconnect between the corporate security and socio-organisational literature in this regard; with the findings of this study supporting the socio-organisational literature perspective.

7.2 Theoretical Implications

The study revealed a significant disconnect between the corporate security and socio-organisational literature. The discourse of a strategic and influential security function within organisations is found to be unfounded; with the socio-organisational literature suggesting the inverse. Consequently, interpretation and discussion of this disconnect has identified a limited appreciation in corporate security texts for the broader organisational stratum of work, with misconceptions and embellishment of the corporate security's importance and function (Fay, 2002; Sennewald, 2011; Cubbage & Brooks, 2013). Significantly, it is identified that there is a misalignment in views of the role of corporate security specialists within organisations; with corporate security overstating its significance and role from the organisational perspective. Furthermore, the interpretation articulates corporate security as an operational and tactical function with a time horizon of five years, severely limiting its impact on strategic matters to the business (Jaques, 1996).

Nevertheless, the implications for the corporate security literature and for professional security education are significant, as the findings contest the current literature consensus. In examination of the literature, many security management texts are written from what could be perceived to be a low level of work (Stratum One-Three), with limited appreciation of the broader organisational context (Barefoot & Maxwell, 1987; Fay, 2002; Fischer, et al., 2008; Sennewald, 2011). Consequently, it could be argued from the interpretation that the positioning of the corporate security function at a lower stratum of work has contributed to this limited discourse. Furthermore, the corporate security literature continues to argue for strategic significance and decision making (McGee, 2006; Sennewald, 2011; Cubbage & Brooks, 2014); however, it is suggested that this argument is inherently flawed by a biased perspective that does not incorporate the broader socio-organisational worldview (Robbins & Judge, 2010). If security specialists want to be elevated into the executive team, then they must shed their highly technical focus, and broaden their understanding of corporate operations and strategic management undertakings.

Accordingly, through application of the socio-organisational literature, the grounding of corporate security as a specialist activity of functional importance to the broader organisation can be argued (Fayol, 1949). Whilst there has been appreciation for this importance throughout the security literature, it has not been clearly articulated where the corporate security function sits within the organisation. Subsequently, literature discourse has suggested that the function is positioned within the concept of support staff; where the provision of indirect support to business activities is undertaken (Talbot & Jakeman, 2009; Smith & Brooks, 2012). On the contrary, the interpretation from this study has indicated that the corporate security function is positioned within the technostructure of an organisation; providing specialist services and analytic advice to safeguard business operations, and shape exposure to the external environment (Mintzberg, 1980; Galbraith, 1985). Therefore, this articulation provides a significant shift in the perception of security activities

as it postulates evidence to support the claim that security is an embedded corporate activity of significance.

7.2.1 Role Articulation

The security literature provides little consistency in the articulation of security roles and levels of work. This inconsistency can be attributed in part to the ill-defined nature and relative immaturity of the corporate security function. By comparison, the significantly more mature socio-organisational literature provides a framework through which the delineation of roles within the corporate security function can be aligned. For example, the interpretation indicates that the corporate security function operates between Stratum One and Stratum Four within the organisational stratum of work. The implications of this finding are significant to the corporate security literature as this role articulation is formulated from an outside perspective; allowing for a more consistent measure that can be used across disciplines. Consequently, the use of the broader socio-organisational literature to measure the corporate security stratum of work suggests a stronger alignment to the actual structure of the function as opposed to the articulation from the internal perspective.

Furthermore, implications of this interpretation include insights into security career progression, alongside the supposed glass ceiling inherent in the function (Coole & Brooks, 2015; Coole, et al., 2015). Significantly, with the inconsistencies in the corporate security functions structure throughout the literature, the findings indicate an underlying stratum of work. This stratum of work, when considered from the broader occupational stratum of work, allows for the mapping of career progression and alignment of job roles and functions. Significantly, understanding the seating of security roles on this stratum ensure consistency, and allows for security education institutions to align learning outcomes and curriculum to their targeted stratum of work.

In addition, the interpretations suggests that the maximum level of work in the corporate security function is indeed Stratum Four; suggesting that there is evidence to support the claim of a glass ceiling in the domain. Subsequently, through an examination of the socio-organisational literature, the argument can be made that this ceiling exists for almost all technical occupational activities of work in organisations. For example, Mintzberg (1973) alongside Jaques (1996) and Robbins and Judge (2010) postulate that higher strata work requires a generalist managerial approach, with limited specialist skills. Consequently, these specialist skills include the application of those core activities identified by Fayol (1949). Therefore, to progress beyond the confines of the business unit and enter the executive stratum of work, individuals must shed their specialist focus and embrace generalist approaches to management.

7.3 Policy Implications

In consideration of the interpretation, significant implications for the development and implementation of policy at education institutions, national institutions, and legislative and regulatory institutions are identified. For instance, through an improved understanding of the roles, functions, and positioning of the corporate security function it is possible to tailor policy engagement, development, and implementation phases more specifically to the targeted demographic.

7.3.1 Education and Training

The study's findings suggest that the corporate security function operates between Stratum One and Stratum Four within an organisation. Consequently, this limits the function to tactical and operational level decision making and associated activities. Significantly, through this articulation of roles, with clear articulated boundaries of work, it is possible to develop more relevant education and training platforms. For example, Stratum One workers operate in a role that require strict operational boundaries; using training and procedures to solve problems in their work. On the contrary, Stratum Four workers operate more abstractly and also rely on managerial skills to conduct their work. Accordingly, through an appreciation of these work types, education platforms could be developed to target specific knowledge, problem solving, and thinking styles inherent in an individual's stratum of work. Furthermore, this insight could allow for delineation between university level education, and vocational training aiding in the identification of instruments, procedures, and abstract concepts as an epistemic model to be taught at specific levels of work.

In addition, the findings suggest that if corporate security practitioners wish to progress beyond their restricted function embedded within the technostructure, they require higher level management education. For instance, due to the considerably more generalist and abstract application of work at the higher levels of an organisation, it is argued that the specialist and specific skill set leveraged by corporate security practitioners is not sufficient to progress beyond the analytical focus of the technostructure (Mintzberg, 1980; Galbraith, 1985). As a result of this finding, it is argued that corporate security practitioners need to understand the function and language of business, alongside embracing generalist managerial practice and process through formal education.

7.3.2 National Institutions and Industry Engagement

Simultaneously, through articulation of the roles within the corporate security function, it is possible to explore the disposition of industry practitioners. Consequently, it is considered that Stratum One workers consist of those occupations that make-up the brunt of corporate security practitioners identified by the Australian Bureau of Statistics (ABS) data collection (Prenzler, 2005). Significantly, this finding is problematic as it indicates that the ABS is not collecting all relevant data when considering the corporate security industry. Thus, the interpretation of the findings suggests that the ABS should consider more practitioners along the occupational stratum of work; being inclusive of corporate security practitioners as they progress along the stratum of work within organisations.

Furthermore, use of the articulation of roles in the corporate security function can aid other national institutions in targeting specific stratums of work when required to engage with the industry. This can ensure that information sharing and discourse is occurring at the appropriate level and will allow national bodies to engage with the right stakeholders in the right context.

7.3.3 Legislative and Regulatory Implications

The findings of this study have the potential to shape legislation and regulation for the corporate security industry. The insight provided by the interpretation to the structure and make-up of the corporate security function could allow for more accurate and relevant legislation and regulation to be adopted by Federal, State, and Local Governments. For example, security licensing in its current form does not accurately depict the broader corporate security stratum of work. Furthermore,

professional bodies such as ASIS, ASIAL and the Australian Security Professional Registry could align their structure and professional acceptance criteria with the identified stratum of work.

7.4 Limitations

Findings from this study must be considered within the limitations of the research which are inherent in both the study design, as well as the analysis of the results. Jaques (1996) theories concerning the time-span of discretion and its relation to an individual's level of work within the occupational strata does have significant support from the literature (Craddock, 2002). However, it is important to note that shifts in globalisation and technology may have considerable impact on its application to modern work environments (Boal & Whitehead, 1992; Ivanov, 2006; Rossi, 2008; Stichweh, 2008). In addition, the decrease in temporal-spatial concerns with the rise of modern technology across all job roles could have significant impacts on the relationship between complexity and time span of discretion (Rossi, 2008). Consequently, it could be argued that complexity has penetrated the lower echelons of organisational work through the adoption of information technology, simultaneously decreasing the time span of discretion required to action tasks. Boal and Whitehead (1992) further suggest that Jaques (1996) theories are only applicable to individuals that are tackling 'tame' problems as opposed to 'wicked' problems, which could impact the theories applicability to the corporate security domain.

Furthermore, criticisms lay in consideration of behavioural traits, as Jaques' (1996) does not consider behaviour to be a contributing factor to an individual's capacity to handle complexity in work. Boal and Whitehead (1992), alongside (Mintzberg, 1973) and the broader literature (Martin & Fellenz, 2010; Robbins & Judge, 2012) consider behavioural traits to be a significant contributor to an individual's work capacity. Moreover, these considerations are especially true in difficult circumstances such as crisis and high impact events (Talbot & Jakeman, 2009), where security individuals are generally responsible.

Additionally, in the application of Jaques' (1996) work, the Task Complexity Measurement Tool (TCMT) and Work Measurement Scale (WMS) were created for the research. Nonetheless, the research instrument indicated an acceptable level of reliability and validity (Chapter Three). However, it is important to touch on the weighting of these tools in the research, and the impacts this had on the analysis. For instance, the analysis was skewed towards the WMS result over the TCMT as this was determined to be more accurately aligned to the cross check data embedded in the research instrument. Additionally, whilst the TCMT was directly adapted from Jaques' (1996) original works, the tool did not translate well into an online survey format. Consequently, as the WMS was created from scratch through the first stage of the study and then relied upon to weight and conduct the analysis, several unforeseen biases or limitations could be present in the findings.

Consideration must also be given to the sample where these tools and analysis was applied. In particular, whilst the corporate security industry is significant in population (Prenzler, 2005; Prenzler et al., 2009), the usable sample size collected (N=33) is not statistically significant. Therefore, criticism of this sample size must be made and is relevant to the findings of the research. Additionally, the sample size could have significantly skewed the study findings due to missed opportunities to penetrate higher strata of work within the industry. Thus, conclusions made in the discussion may be subject to change if the research is conducted on a statistically valid sample.

7.5 Recommendations

The study presents significant findings to the corporate security literature, broader academia, industry, government, and regulatory bodies. Consequently, whilst some limitations are identified in the research, the implications of these findings must be sincerely considered going forward. Therefore, it is suggested that numerous steps be taken in future research, namely;

1. Study replication; specifically to increase the sample size to allow for statistically valid generalisation;
2. Review of the corporate security function; specifically an exploration of each identified stratum of work in aid of establishing functional boundaries and specific roles;
3. Investigate the alignment between security education curriculum and the identified stratum of work; specifically that between prescribed training and procedures at lower strata, and abstract concepts at higher strata;
4. Investigate and consider career progression pathways along the identified stratum of work; specifically those of graduates;
5. Further research into the corporate security functions alignment to the technostructure; specifically aligning outputs and functions with this embedded activity of organisational work;
6. An extensive review of the corporate security literature must be undertaken in light of the findings of this study; and
7. Further research into the time-span of discretion measurement, specifically it's application in modern times to modern organisations.

7.6 Conclusion

Corporate security is a significant organisational activity that provides for the protection of people, information and assets within an organisation; alongside the self-protection of a corporation (Fayol, 1949; Smith & Brooks, 2012). Consequently, the ability to understand, measure, and define such a practice area can have important implications for academia, industry, governments, regulatory and industry bodies, and the broader community. Nonetheless, corporate security remains an ill-defined and nebulous term and practice area in the literature, with an ambiguous body of knowledge (Smith & Brooks, 2012; Brooks & Corkill, 2014). In addition to this ambiguous nature, corporate security is struggling through a process of professionalisation with strong evidence against its professional claim (Coole, Brooks & Treagust, 2015). Subsequently, many security practitioners are misaligned on the corporate stratum of work; assigned responsibilities not befitting their experience, capacity to work, or even their job title alignment (McGee, 2006; Sennewald, 2011).

Significantly, this study investigated the corporate security stratum of work within organisations, revealing the positioning of this function within business activities, but also identifying several strata of corporate security work. For instance, this study found corporate security works to be conducted at the lower strata of an organisation, between Stratum One and Stratum Four . These work levels are focussed operationally and tactically within organisations, providing specialist knowledge and experience to more concrete, actionable problems (Jaques, 1996). Subsequently, this finding contests the corporate security consensus, which purports the existence and necessity of a strategic

corporate security practitioner, championing the security cause at the highest levels of an organisation (Sennewald, 2011; Cubbage & Brooks, 2013).

On the contrary, findings clarify the corporate security function as a business operator within the organisations technostructure, which provides analytical advice to influence exposure to the external operating environment (Fayol, 1949; Mintzberg, 1980). This influence in shaping exposure firmly roots technostructure functions to non-executive roles within an organisation, as adaptation to a constantly changing operating environment requires quick decision making within the tactical and operational time-span (Mintzberg, 1980). Axiomatically, corporate security leverages its specialist skill set within this time-span to ensure business operations are not adversely affected by the security risk inherently found in the external operating environment.

Accordingly, these findings have significant implications for academia, industry, and other bodies, especially due to the serious divergence uncovered through the alignment of the corporate security literature to the broader socio-organisational literature. Such divergence suggests that academia must further investigate the corporate security function from a managerial perspective to discover the full extent of this disconnect, whilst also addressing the invalidated consensus. Furthermore, industry bodies can harness the findings of these studies to identify career pathways, uncover barriers to progression beyond the operational and tactical levels of the technostructure, and compare roles both between organisations and functional domains. Finally, other bodies can embrace these findings in the development of legislation, regulation, and education curricula to greater align with the established corporate security stratum of work.

REFERENCE LIST

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

Atlas, R. I. (2008). *21st century security and CPTED: Designing for critical infrastructure protection and crime prevention.* Auerbach Publications. Retrieved from http://ECU.eblib.com.au/

Australian Bureau of Statistics. (2014). Population by age and sex, regions of Australia (Cat. No. 3235.0). Retrieved from http://www.abs.gov.au/

Barefoot, J. K., & Maxwell, D. A. (1987). *Corporate security administration and management*. Boston: Butterworth Publishers.

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

Boal, K. B., & Whitehead, C. J. (1992). A critique and extension of the stratified systems theory perspective. In R. L. Phillips & J. G. Hunt (Eds.), *Strategic leadership a multiorganizational-level perspective*. Westport, CT: Quorum Books.

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., & Coole, M. (2011). *Mapping the organisational relations within physical security's body of knowledge: a management heuristic of sound theory and best practice*. Paper presented at the 4th Australian Security and Intelligence Conference, Perth, Australia.

Brooks, D., & Corkill, J. (2014). Corporate security and the stratum of security management. In K. Walby & R. K. Lippert (Eds.), *Corporate security in the 21st century : Theory and practice in international perspective* (1st ed., pp. 216-234) Hampshire, UK: Palgrave Macmillan.

Cason, K., & Laurents, M. D. (2006). A modest proposal: A testable differentiation between third-and-fourth-order information complexity. *International Journal of Applied Psychoanalytic Studies, 3*, 4.

Chilcott, J. (1998). Structural functionalism as a heuristic device. *Anthropology & Education Quarterly, 29*(1), 103-111.

Christensen, L., & Johnson, R. B. (2014). *Educational research quantitative, qualitative and mixed approaches* (5th ed.). London: SAGE Publications.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91-150. doi:10.2307/1147596

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

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(August), 588-508.

Coole, M. (2010). *Theory of entropic security decay: the gradual degradation in effectiveness of commissioned security systems.* (Masters Thesis). Retrieved from http://ro.ecu.edu.au/theses/372

Coole, M., & Brooks, D. (2015). Towards security professionalisation: The cultural journey to employ and develop future security professionals. *Australian Security Magazine, APR/MAY,* 22-23.

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

Coole, M., Corkill, J., & Woodward, A. (2012). *Defence in depth, protection in depth and security in depth: A comparative analysis towards a common usage of language*. Paper presented at the 5th Australian Security and Intelligence Conference, Perth, Western Australia.

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.

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

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

Durkheim, E. (1984). *The division of labour in society* (W. D. Halls, Trans.). Basingstoke: Macmillan.

Fay, J. J. (2002). *Contemporary security management* (1st ed.). MA: Butterworth-Heinemann.

Fayol, H. (1949). *General and industrial management*. Chicago: Pitman Publishing Corporation.

Fennelly, L. J. (1997). *Effective physical security* (2nd ed.). Newton, MA: Butterworth-Heinemann.

Fetterman, D. M. (2008). Ethnography. In L. M. Given (Ed.), *The SAGE Encyclopedia of Qualitative Research Methods* (pp. 289-293). Thousand Oaks, CA: SAGE Publications, Inc.

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

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

Galbraith, J. K. (1985). *The new industrial state* (4th ed.). Boston: Houghton Mifflin Company.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Burlington, MA: Butterworth-Heinemann.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Sydney: Butterworth-Heinemann.

Gould, D. P. (1986). Stratified systems theory in the design of organization-wide information systems. *International Jounral of Information Management, 6*(1), 5-15.

Griffiths, M., Brooks, D., & Corkill, J. (2010). *Defining the security professional: definition through a body of knowledge*. Paper presented at the 3rd Australian Security and Intelligence Conference, Perth, Australia.

Grobler, S. W. (2005). *Organisational structure and Elliott Jaques' stratified systems theory.* (Masters Degree in Business Leadership), University of South Africa, South Africa. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/146/2005%20MBL%203%20Research%20Report%20S%20W%20Grobler.pdf

Hillman, S. (2011). Physical Security 101: Evolving 'defense in depth'. *InTech, 58*(3), 28-31.

Hooijberg, R., & Quinn, R. E. (1992). Behavioral complexity and the development of effective managers. In R. L. Phillips & J. G. Hunt (Eds.), *Strategic leadership a multiorganizational-level perspective*. Westport, CT: Quorum Books.

Interim Security Professional's Taskforce. (2008). *Advancing security professionals*. Australia: Security Professionals Australasia

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).

Jacobs, O. T., & Lewis, P. (1992). Leadership requirements in stratified systems. In R. L. Phillips & J. G. Hunt (Eds.), *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* (1st ed.). London: Heinemann Educational Books Ltd.

Jaques, E. (1970). *Equitable payment a general theory of work, differential payment, and individual progress* (2nd ed.). London: Heinemann Educational Books Ltd.

Jaques, E. (1972). *Measurement of responsibility a study of work, payment, and individual capacity*. New York: John Wiley & Sons Inc.

Jaques, E. (1976). *A general theory 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: Cason Hall and Co Publishers.

Jaques, E. (2002). *The life and behavior of living organisms a general theory*. Westport: CT: Praeger Publishers.

Lee, W. J., Rainey, H. G., & Chun, Y. H. (2010). Goal ambiguity, work complexity, and work routineness in federal agencies. *The American Review of Public Administration, 40*(3).

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

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

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

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.

Mintzberg, H. (1973). *The nature of managerial work* (1st ed.). New York: Harper & Row, Publishers, Inc.

Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. *Management Science, 26*(3), 322-341. Retrieved from http://www.jstor.org/stable/2630506

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.

Nunes-Vaz, R., Lord, S., & Ciuk, J. (2011). A more rigorous framework for security-in-depth. *Journal of Applied Security Research, 6*(3), 372-393.

O'Byrne, D. (2013). *Introducing Sociological Theory* Retrieved from http://ECU.eblib.com.au/

Parsons, T. (1951). *The social system*. London: Routledge.

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*.

Prenzler, T., & Milroy, A. (2012). Recent inquiries into the private security industry in Australia: Implications for regulation. *Security Journal, 25*(4), 342-355.

Prenzler, T., Sarre, R., & Earle, K. (2008). Developments in the Australian private security industry. *Flinders Journal of Law Reform, 10*(3).

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

Roberts, K. (2012). *Sociology: An introduction* Retrieved from http://ECU.eblib.com.au/

Rossi, I. (2008). Toward a framework for global communication: Durkheim, phenomenology, postmodernism, and the "construction" of place and space. In I. Rossi (Ed.), *Frontiers of Globalization Research* (pp. 133-151). New York: Springer.

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

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.

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

Smith, C. (2003). *Understanding concepts in the defence in depth strategy.* Paper presented at the Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference.

Smith, C., & Brooks, D. (2012). *Security science: The theory and practice of security* Retrieved from http://ECU.eblib.com.au/

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*. USA: ASIS International.

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

Standards Australia. (2006). Security risk management (HB167-2006). Retrieved from http://www.standards.org.au/

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.

Talbot, J., & Jakeman, M. (2009). *Security risk management body of knowledge*. New Jersey: Wiley.

Weissenberg, P. (1971). *Introduction to organizational behavior*. Scranton, PA: International Textbook Company.

White, J. (2014). *Security risk assessment managing physical and operational security* (1st ed.): Butterworth-Heinemann.

White, R., Haines, F., & Asquith, N. (2012). *Crime & criminology* (5th ed.). South Melbourne, Victoria: Oxford University Press.

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

APPENDIX A: WORK MEASUREMENT SCALE

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?								

APPENDIX B: TASK COMPLEXITY MEASUREMENT TOOL

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		Disagree	Agree		Very Strongly Agree
1. 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
2. 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
3. My work requires planning for future in consideration of current needs, as well as develops alternative plans as a backup.		2	3	4	5	6
4. 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
5. 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
6. 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
7. 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 C: SURVEY INSTRUMENT

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?

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 D: SURVEY QUESTION CHANGES

Original Question	New Question
Work Measurement Scale	
In what time frame do you plan for the future?	At work, how far into the future do you plan ahead?
In what time frame do you allocate resources into the future?	At work, how far into the future do you allocate resources?
How far into the future is your longest work assignment?	How far into the future is your longest task deadline?
	What is the longest time frame you allocate a subordinate to complete a task?
In what time frame do you expect financial return on investments?	At work, when do you expect return on investment for allocated resources?
How far into the future are you planning the development of staff? (Training, Experience)	Removed
Task Complexity Measurement Tool	
My work is done by following an assigned plan to a goal, over-coming obstacles by direct actions and trial-and-error	My personal work requires overcoming obstacles by direct actions, trial and error
My work involves collecting information about a defined problem, and using that information to develop a solution or make a decision.	My personal work requires collecting information about a regular problem to develop a solution
My work requires planning for future n in consideration of current needs, as well as develops alternative plans as a backup.	My personal work requires developing alternative backup plans
My work requires the management of a number of projects which must be adjusted and undertaken in relation to each other	My personal work manages multiple projects simultaneously
My work requires an understanding of the immediate and downstream consequences on my organisation if any aspect of a project is changed.	My personal work requires consideration of the downstream supply chain consequences
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	My personal work requires me to influence the environment outside of my organisation that may be significant to strategic objectives
My work requires the development of world-wide strategic options and the creation of business units, by growth, acquisition, mergers and joint ventures	My personal work requires the creation of business divisions, by growth, acquisition, mergers and joint ventures

APPENDIX E: SURVEY RESPONSES

Job Titles of Respondents	Number of Employees Managed	Job Level	WMS Result	TCMT Result	Assessed Level of Work	Average Level of Work	Standard Deviation
Stratum I							
Business Proprietor	3	IV	I	VI	I	3.67	2.05
Security/Comms Technician	1	I	I	IV	I	2.00	1.41
Not Assessed	NA	I	I	VII	I	4.33	2.83
Sales and Technical Support	0	I	I	IV	I	1.75	1.41
Not Assessed	1	IV	I	V	I	3.33	1.7
Not Assessed	0	I	I	I	I	1.00	0
Assistant Director	10	III	I	IV	I	2.67	1.25
CEO	15	VII	I	VII	I	4.67	2.83
Not Assessed	1	NA	I	VI	I	3.50	2.5
Not Assessed	NA	II	I	NA	I	1.50	0.5
Consultant	3	VII	I	VI	I	4.67	2.62
Stratum II							
Security Coordinator	50	III	II	VII	II	4.00	2.16
Country Security Manager	20	IV	I	IV	II	3.00	1.41
Associate Security Consultant	3	III	II	IV	II	3.00	0.82
Not assessed	NA	V	II	IV	II	3.67	1.25
Principal Consultant – Security & Risk	0	I	II	VI	II	3.00	2.16
Senior Consultant, Crisis & Security Consulting, Middle East	0	NA	II	V	II	3.50	1.5
Not Assessed	NA	II	II	V	II	3.00	1.41
Not Assessed	6	III	I	IV	II	2.67	1.25
Not Assessed	4	IV	II	VI	II	4.00	1.63
Security Coordinator	0	III	II	IV	II	3.00	0.82
Not Assessed	NA	I	II	VI	II	3.00	2.16
Not Assessed	60	III	II	VII	II	4.00	2.16
Stratum III							
Lead Security Consultant	0	III	III	II	III	2.67	0.47
Security Program Manager	0	III	III	IV	III	3.33	0.47
Security Manager	8	III	III	IV	III	3.33	0.47
Security Professional	0	I	III	VI	III	3.33	2.05
Not Assessed	30	III	II	IV	III	3.00	0.82
Not Assessed	30	IV	III	VII	III	4.67	1.7
Director – Adjunct Ass Prof	0	VII	III	IV	III	4.67	1.7
Stratum IV							
Not Assessed	5	III	IV	V	IV	4.00	0.82
Not Assessed	100	VII	IV	VII	IV	6.00	1.41
National Security Director	90	V	IV	VI	IV	5.00	0.82
Not Assessable							
Business Development Manager	NA	V	NA	NA	NA	NA	NA
Not Assessed	NA	I	NA	NA	NA	NA	NA
Chief Operating Officer	700	VII	NA	NA	NA	NA	NA
Manager Commercial Security	5	III	NA	NA	NA	NA	NA

Note: NA = Not Assessed