7-18-2019

Corporate security career progression: A comparative study of four Australian organisations

Codee Roy Ludbey
Edith Cowan University

David J. Brooks
Edith Cowan University

Michael Coole
Edith Cowan University

10.1057/s41284-019-00189-3

This is a post-peer-review, pre-copyedit version of an article published in Security Journal. The final authenticated version is available online at: https://doi.org/10.1057/s41284-019-00189-3

Ludbey, C. R., Brooks, D. J., & Coole, M. (2020). Corporate security career progression: A comparative study of four Australian organisations. *Security Journal, 33*(4), 531-551. https://doi.org/10.1057/s41284-019-00189-3

Corporate security career progression: A comparative study of four Australian organisations

Codee Roy Ludbey, Edith Cowan University

David Brooks, Edith Cowan University

Michael Coole, Edith Cowan University[1]

Abstract

The study investigated the Corporate Security stratum of work within large Australian organisations, seeking to extract professional seating, roles, associated task complexity, career opportunity and progression ceilings as articulated through the socio-organisational literature. Two phases were applied: Phase One used online surveys distributed to participants (N=53) across four Australian organisations, Phase Two employed semi-structured interviews and focus groups (N=14).

Findings reinforced the established literature articulation of corporate security's roles; however, they contested the current articulation of corporate security's executive level seating within large organisations. Instead, the study identified a Corporate Security seating with a restricted sphere of risk-based influence, along with a maximum career level at general manager. The study demonstrates an occupational corporate security ceiling, debunking the security executive belief. Corporate Security was located within the technostructure group as a specialist, limiting opportunity for executive level roles or strategic influence.

Keywords: Organisation, Career, Occupation, Stratum, Work, Complexity, Security, Glass-ceiling

Introduction

Large corporate organisations are complex entities comprised of systematic arrangements of individuals and processes aligned to achieve defined business objectives (Weber, 1947; Litterer, 1963 p. 5). Today, these organisations and its individuals (or occupations) are subject to increasing complexity to meet the modern challenges of society (Oesch, 2015; Stichweh, 2008). Such increasing complexity relates to the requirement for modern organisations to tackle the amplified uncertainty of the globalised information age in a timely manner to manage risk exposure (Stichweh, 2008; Clement, 2015). Subsequently, organisational structures are shifting from rigid hierarchical constructions to rich networks of individuals, aligned horizontally and vertically, to improve their capacity to understand their operating environment and respond to market demands and societal pressures (Barnes, 1995 pp. 193-222).

The author acknowledges the Australian Government for its support in the conduct of this research through the Australian Government Research Training Program Scholarship.

Such organisational challenges have historically included security concerns, particularly due to the requirement for the organisation to self-police and protect its operations from internal and external harm (Fayol, 1916; 1949). Nevertheless, security considerations are changing as modern organisations witnessa shift in threat drivers and reduced societal risk tolerances (Beck, 1992). As Beck (1992) and Füredi (2006) articulates, manufactured risks, foreseeable risks and unforeseeable risks are becoming less acceptable by society, and organisations are forced to shift their risk acceptance accordingly. Consequently, organisations are relying on specialised occupations to address these societal expectations; creating a demand for labour differentiation and further sub-specialisation to manage these ever-growing risks (Krahmann, 2011). As Giddens (1991, p. 17) explains, the real difference between modern and traditional organisations is the "concentrated reflexive monitoring they both permit and entail" by way of these differentiated specialist occupations. Such reliance on these occupations results in an increased level of seniority for practitioners and consequently a broadened work stratum.

Therefore, the use of individuals within occupations to manage such broad organisational risk infers a link between the capacity of a person to manage their operational and environmental complexity, and their organisational seating (Clement & Clement, 2013). As Jaques (1996) noted, individuals who understand and address uncertainties in their organisational environment, and subsequently manage risk over longer and longer periods of time, tend to align with higher level roles within organisations. Nevertheless, with the impact of modern technology, the time available for organisations to make decisions in such uncertain environments is reduced, while concurrently enabling entities to collect more information than ever before (Ivanov, 2011; 2015). Accordingly, it is argued such factors are changing the equation for occupational success (Craddock, 2002; Le Grand & Tahlin, 2013; Maitland & Sammartino, 2014). These changes have shifted the status and perception of specialised occupations who manage uncertainty and reduce risk, elevating those that enable organisations to conduct profit-making activities in a managed environment.

Acknowledging that such risk management occupations vary in their sub-specialisation, modern corporate risk reduction includes the use of Corporate Security (Willis, 2007). Corporate Security is defined as a business utility that provides a self-protection function embedded within an organisation that aims to reduce harm manifestations against people, information, and physical assets from threat (human) actors (Smith & Brooks, 2012). In the achievement of corporate objectives, security was historically seen as a lower stratum undertaking, associated with simple loss reduction techniques to reduce theft losses as a simple guardian (Burnstein, 1978; Barefoot & Maxwell, 1987).

A reflection on organisational maturity highlights that the complexities of modern society have shifted organisational approaches to market, and the associated workforce that fulfils the roles to achieve organisational objectives. As a result of such societal shifts, Corporate Security is undergoing a change away from its previous '*simple guardian*' role toward a holistic organisational protection function, fulfilling an enterprise risk management responsibility to facilitate the achievement of objectives (Talbot & Jakeman, 2009). Thus, one must consider how occupations may succeed in this new environment, particularly where traditional approaches and perceptions may no longer apply (Oesch, 2015; Speer, 2017).

While profit making activities remain the core value in modern capitalist organisations, competing values aligned to ethical and moral conscious also impact modern business and influences decisions and corporate direction (Clarke, 2015). Such changes result in career uncertainty for many workers, their future roles, career progression, and potential pathways to senior executive levels are impacted with ceilings of career progression that have existed in the past shifting, and new ones being put in place in response to market demands (Freidman, Laurison, & Miles, 2015; Koch, Forgues, & Monties, 2015). It follows that these new organisational environments affect specialist occupational pathways, including Corporate Security, and thus the study sought to understand this phenomenon. The study sought to respond to the question: *To what extent, if any, does the Australian corporate environment have a career progression ceiling for security practitioners?*

Security Work in Organisations

The Weberian (1947) view of organisation, braced by others such as Mintzberg (1979), expresses several forms of systemic structures of individuals, such as the bureaucratic, professional, representative democratic, postmodern and network forms. Within these forms, Diefenbach and Sillince (2011) posit that hierarchical structures exists either in a formal or informal capacity. Within these hierarchical structures work is stratified (Jaques, 1976). Mintzberg (1980) examined several of these organisational forms and identified core structures kin to each, inherent in all organisational forms. Consequently, these elements comprise the structural basis of organisational stratification (Meyer & Rowan, 1977; Rowbottom & Billis, 1977).

The organisational structures identified by Mintzberg (1980) include:

- Strategic Apex, which comprises executive decision makers who guide and lead the organisation;
- Middle Line, which contains general managers and supervisors who translate the strategic direction, articulated by the strategic apex, into operational activities to be conducted by the operating core;
- Operating Core, who fulfil the core business functions and render services or create products for the market;
- Support Staff, who provide specialist internal focussed services in support of the core business activities such as human resources; and
- Technostructure, which provides specialist external focussed services to reduce uncertainty and shape the operating environment in support of business activities.

The general form of these organisational structures is depicted in Figure 1.

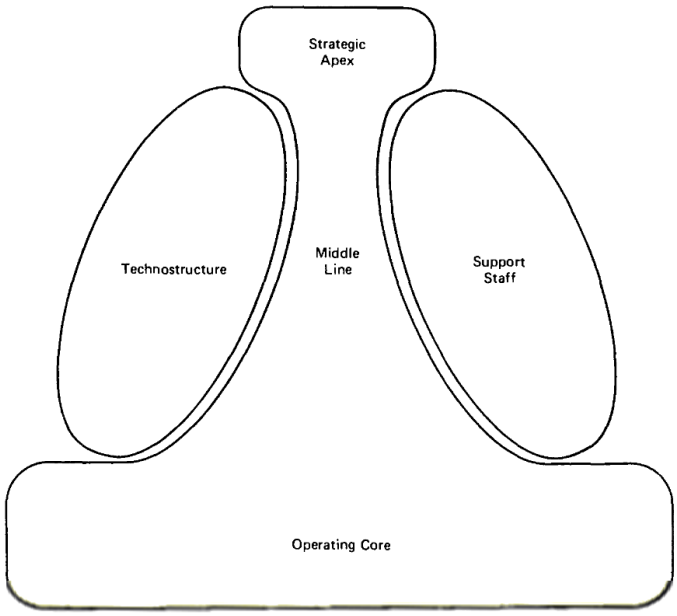

Figure 1. General Framework of Organisational Forms (Mintzberg 1980; Martin & Fellenz, 2010)

Where the organisation determines it is required, the Corporate Security occupation sits within this organisational structure. Corporate Security is a distinct occupation, separate from national security and private security occupations. National security occupations are oriented to defence, government, and policing roles, and in contrast, private security occupations are generally contracted goods and services. Corporate Security roles are in-house, reflexive and focus on organisational uncertainty and risk reduction (Petersen, 2014; Prenzler, Earle, & Sarre, 2009; Sarre & Prenzler, 2000; Walby, Wilkinson, & Lippert, 2014).

Subsequently, Corporate Security's role of risk management is achieved within, and through a stratified hierarchy of roles and responsibilities (Bamfield, 2014; Fay, 2002; Nalla & Morash, 2002; Sennewald, 2011; Wakefield, 2014). These occupational roles include the security officer, investigator, surveillance operator, technicians, systems administrators, supervisors, security managers and chief security officers, amongst others, and are broadly categorised as executive security roles, security manager roles, security supervisor roles, and security officer roles (Barefoot & Maxwell, 1987; Brislin, 2014; Brooks, 2013; Gill & Howell, 2012; Nalla & Wakefield, 2014).

Various authors (see, Nalla & Morash, 2002) have suggested that security is a senior, executive, organisational function that liaises with the executive strata. They argue that such senior security roles consist of shaping business decisions through a security lens, allowing the business to operate securely and make decisions informed by security risk management (Talbot & Jakeman, 2009). The concept of an executive level security function is further supported by Ocqueteau (2012), who suggested that the majority of security directors for large corporations have their direct superior in the executive committee, situating security at the peak of organisations. Bamfield (2014) further supported this view, postulating that such a role—the Chief Security Officer—should exist to develop companywide strategy and policy in the protection of organisation's assets and operations. These roles should then delegate responsibilities and define the security strategy for implementation through a managerial stream.

Such a managerial stream would be considered a 'security manager' role, responsible for a specific, or several specialist security areas (Bamfield, 2014). While security managers seem to be shifting away from a defined technical specialty i.e., shifting from a technical appreciation of physical security towards a more generalist staff managerial role, they are considered generalists within the security domain (Brooks & Corkill, 2014). For example, security managers need to understand the organisational operating context, threat drivers to objectives, security strategy, and the role and limitations of security technology along with broader management requisites including company policy, local laws and regulations, and resourcing and management fundamentals to name but a few (Barefoot & Maxwell, 1987; Fay, 2002). Functionally, security managers direct and lead smaller teams of technical security employees, overseen by security supervisors.

Security Career Progression

Within such a stratified work hierarchy, questions regarding career progression opportunities arise, and how do specialist personnel progress in relation to other identified workers who are aligned to other parts of the organisational structure? Strauss (1975/2001) found several progression pathways for occupations within large organisations. Specifically, roles more closely aligned to profit-making activities (the Operating Core, Middle Line, Strategic Apex) see more career success and higher likelihood of reaching their work hierarchy peak than those occupations that fulfil specialist tasks. Koch et al., (2015) and others (Heslin, 2005; Speer, 2017) support this position, supposing that this progression relates to the type of human capital accrued throughout the individual's career and subsequent rewards for this capital.

Sammarra, Profili and Innocenti (2012) explain that occupations fulfilling profit-making roles require substantial organisation specific knowledge, and thus this experience is rewarded with managerial positions and hierarchical progression. In contrast, occupations which fulfil specialist functions do not necessarily require this organisation specific knowledge, and thus attract different incentive schemes (Jesus, Seibert, Kraimer, Wayne, & Liden, 2015). For example, it is argued that technostructure roles apply their expertise from an independent body of knowledge that can be applied across organisational contexts, and thus do not need to accrue or apply substantial organisation specific expertise.

With career progression, Mumford, Campion and Morgeson (2007) explain that organisations seeking to promote individuals in the hierarchy also reward the application of generalist managerial skills, as opposed to technical skills. As organisational problems become more unstructured, they are managed by higher order work streams, and individuals solving these problems at more senior levels of work apply more unstructured and generalist skills (Clement & Clement, 2013). Such progression is also supported by education, with higher levels of education aiding career upgrades (McGregor, 1997; Speer, 2017).

Within the Corporate Security context these elements are just as vital, where Brooks and Corkill (2014) articulated similar progression along the security occupation pathway. Security practitioners move away from the application of technical skills toward generalist managerial skills as their career progresses. Nevertheless, it is proposed that while this holds true, the problem being solved by senior security practitioners with this generalist work approach

is still wholly within the specialised security domain (technostructure), and not truly aligned with profit making activities or broader business objectives (Coole, Brooks, & Minnaar, 2017; Ludbey et al., 2018).

Measuring the Work Hierarchy

In consideration of these factors in career progression, a measure of work was used to investigate Corporate Security's stratum of work in Australia. Jaques (1996) argued one means of work measure is an individuals' time span of discretion, which is considered their capability to exercise judgement over a period of time in pursuit of an organisational goal. Paired with this measure is task complexity, which relates to the difficulty and uncertainty inherent to any task. By reviewing both of these factors, an individual's indicative level of work for a role can be determined (Ivanov, 2011; Jaques, 1996; Lee, Rainey, & Chun, 2010).

In support of this approach, Le Grand and Tahlin (2013) investigated the components of the wage-profitability equation to understand which factors were significant in role rewards. Le Grand and Tahlin (2013) argued that efficiency related considerations i.e., capacity to handle complexity and judgement, are key differentiators in the hierarchical position along the stratum of work. Such a review of productivity aligns closely with Jaques (1996) understanding of the work. Subsequently, an overall stratum of work can be applied across the identified organisational structures (Table 1). It was proposed that this hierarchical arrangement, paired with the assessment methodologies presented by Jaques (1996), allow for Corporate Security roles to be studied and ranked to determine their overall strata of work within organisations.

Table 1.

Occupational stratum of work in organisations (Jaques, 1996; 2002)

Stratum	Time-Span of Discretion	Role Complexity	Employee Role
Seven	20+ years	Extrapolative Development of Whole Systems	CEO
Six	10 to 20 years	Defining Whole Systems	Executive Vice President
Five	5 to 10 years	Shaping Whole Systems	Business Unit President
Four	2 to 5 years	Transforming Systems	General Manager
Three	1 to 2 years	Task Extrapolation	Unit Manager
Two	3 months to 1 year	Task Definition	First Line Manager
One	1 day to 3 months	Concrete Shaping	Front Line Workers

Methodology

The study investigated the corporate security departments within four large Australian organisations, where three are listed on the Australian Securities Exchange index S&P/ASX 100, and one on the European EuroNext Paris index. Organisations were purposively selected using known contacts, and the Corporate Security departments within each exposed to the two-phase study. Purposive sampling was undertaken in this study to maximise access

to all levels of the corporate security departments which agreed to participate in the study. The researchers were known to the senior security practitioners within these organisations and thus, it was determined that such a sampling choice would be the most practical. Nevertheless there are limitations in this approach, as it is not a randomly selected sample; however, to minimise bias findings, organisations across four separate market areas were chosen.

Subsequently, Organisation One operated in the retail sector of the Australian labour market. The organisation is listed as a top 200 organisation on the Australian Securities Exchange by significance, with over $40 Billion AUD in assets. The organisation employs over 2,500 individuals in their workforce. Organisation Two is a large Australian national banking institution founded in the 1800s. The organisation has an annual income of over $8 Billion AUD, with a workforce that consists of over 35,000 individuals. Furthermore, the organisation is also in the top 200 Australian companies as listed on the Australian Securities Exchange.

Organisation Three was a significant private defence industry organisation founded in 2000, which operates in Australia as an independent subsidiary of a larger multi-national firm. The firm is listed on Euronext, a European stock exchange. This organisation has a revenue that exceeds $1 Billion AUD and employs over 3,000 individuals. Organisation Four was a gaming and entertainment organisation , also listed in the top 200 companies on the Australian Securities Exchange, and with a revenue of over $2 Billion AUD and over 8,000 employees.

Phase One of the study used online surveys (N=368) distributed to the security departments across the four participating organisations, with a response rate of 14% (N=53). The survey instrument (Table 2) used in this study was developed in previous research (Ludbey, 2016), which consisted of a *Task Complexity Measurement Tool (TCMT)*, *Work Measurement Scale (WMS)* and confirmatory check questions (*Self Measure*). Importantly, these instruments were derived from the underlying theory of Jaques (1996) General Theory of Managerial Hierarchies, and have been tested in previous research (Ludbey, 2016; Ludbey & Brooks, 2017; Ludbey et al., 2018). An extract from the Phase One survey is shown below.

Table 2.

Extract of Phase One: Survey

	1 day–3 months	3 months–1 year	1–2 years	2–5 years	5–10 years	10–20 years	20+ years	n/a
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?								

Phase Two consisted of semi-structured interviews and focus groups with participants from three of the four organisations. One organisation (Organisation Three) did not participate in the semi-structured interviews and focus groups due to the inaccessibility of participants during the interview collection period. Nevertheless, the interviews and focus groups (N=14 participants across N=6 focus groups) included executive, middle management and operational security staff based on Jaques work. The questionnaire was developed from the analysis of the Phase One findings, to support, refute and interpret findings in the previous phase. The

questionnaire investigated occupational success, organisational complexity and career progression (Table 3). Table 3 presents an extract of the questionnaire.

Table 3.

Extract of Phase Two: Questionnaire

	Question	Purpose
Occupational Success	Could you explain how you started work in the security industry?	A broad background question will provide some understanding of sociological influences on work and career choices.
	Could you explain your work experience?	Understand Experiential requirements for current role, as well as gather broader sociological information about possible class background.
	Can you talk about the duties you undertake in your role?	Understand role makeup, impact, and purpose.
	Could you elaborate on the value security brings to your organisation?	An understanding of the perceived value that security brings to the organisation could indicate the alignment of security to profit, and thus, success.

Reliability and Validity

In consideration of reliability and validity of the results in Phase One, a cross-organisation comparative test was undertaken using the Kruskal-Wallis non-parametric measure (Field, 2013; Witte & Witte, 2017). A statistically significant result on any of the measures (WMS, TCMT, Self-Measure) indicated that the sample from each organisation are part of the same occupational population (Field, 2013). The data were analysed, with the Work Measurement Scale demonstrating significance ($p=0.06, < .10$) with the TCMT ($p=0.40, < .10$) and Self Measure ($p=0.47, < .10$) results not demonstrating significance. Furthermore, when considering a Spearman Rank-Order Correlation (Witte & Witte, 2017) between all data collected between organisations, the WMS and TCMT pair was statistically valid, as was the WMS and self-assessment measure (WMS:TCMT - $R=0.34$, $P=0.03$; WMS:Self Assess - $R=0.36$, $P=0.02$). The TCMT and self-assessment pair was not statistically significant across all organisations (TCMT: Self Assess - $R =0.04$, $P=0.92$). As such, the statistical tests indicate that the WMS score is the most reliable, and thus this score was used to determine the stratum of work within each participant organisation.

In review of reliability and validity for Phase two, as articulated by Stewart, Shamdasani and Rook (2007, pp. 118-125) consistency in data collection and analysis are paramount in focus group methodological approaches due to the variety of responses possible from participants. To address consistency, the focus group participants were asked the same questions developed from the preceding phase, with subsequent prompting in accordance with semi-structured interview techniques (Qu & Dumay, 2011). Further, a consistent analytical process was undertaken during coding (Saldana, 2009).

Results

Phase One: Task & Work Survey

Due to the outcome of the statistical tests participant responses were scored against the Work Measurement Scale (WMS) score as opposed to the average, self-assessment, or task-complexity measurement tool.

Organisation One, a retail and property group, had identified individuals' level of work operating between Stratum One to Stratum Four using the WMS scoring measure. The data identifies one (5%) participant operating as a Stratum Four employee, with 6 (32%) assessed at Stratum Three, ten (53%) assessed at Stratum Two and 2 (11%) assessed as Stratum One. Of the listed job titles, nine used the term *manager*, with only four responses indicating *first line* or *supervisory* roles. Organisation Two, a banking firm, had individuals identified as operating between Stratum Two to Stratum Three. Three (60%) participants were assessed at Stratum Three and two (40%) were assessed at Stratum Two. Job titles were *management* related.

Organisation Three was a defence industry organisation, with individuals assessed between Stratum One to Stratum Four using the WMS scoring measure. Two workers (33 %) were assessed to be at Stratum Four, followed by two (33%) as Stratum Two, and two (33%) at Stratum One. Job titles were a mix of *management* and *operational*, with three responses not providing a management title. Organisation Four was a gaming and entertainment entity, with individuals being assessed as operating between Stratum One to Stratum Three. One (11%) participant was assessed as a Stratum Three employee and two (22%) as Stratum Two, with the remaining six workers (67%) assessed as Stratum One. Job titles were a mix of *management* and *operational* task roles, with three responses not providing a management title.

It was noted that more operationally focussed corporate security teams, such as that found in Organisation Four (gaming and entertainment), had some senior managerial role titles appear in Stratum One positions (i.e. Director). It is speculated that this occurred due to the legislative nature of gaming and the resulting need for the responsive requirements of such a team, i.e. having to monitor CCTV and respond to incidents immediately on the gaming floor or at alcohol serving outlets. Organisation One (Retail) also had the majority of roles at Stratum Two, which suggests customer-focussed security teams tend to be more operationally focussed. In juxtaposition, Organisation Two (banking) and Organisation Three (defence) had a more senior weighting in their identified roles, suggesting a less operational focus in their tasking.

Phase Two: Interviews & Focus Groups

Phase Two undertook interviews and focus groups, which extracted themes relating to how security careers commence, complexity of work in how practitioners apply their skills within their corporate organisation and career progression.

Occupational Success

The majority of participants started their career in an aligned discipline such as policing or military occupations, or began their career in another area of the security domain before transitioning into a corporate security role (n = 10). While some participants were from other backgrounds, these appeared to be the exception to a strong trend of 'non-civilian' backgrounds. Moreover, the findings uncovered three categories of security roles, which included those operational security roles that involve 'concrete shaping' tasks that are highly process driven (Clement, 2015), as well as professional roles and tactical roles. Professional roles involved the formulation of new approaches and methodologies within a bounded operating environment (Ivanov, 2015). Finally, tactical roles were more aligned with general managerial tasks, including a strong focus on shaping the direction of the security function within the business, focussing on protecting the organisation as whole (Craddock, 2002). Peak security roles did not appear to involve traditional strategic managerial taskings such as detailed market analysis, product generation, or broader business planning (Papadakis & Barwise, 2002).

Organisational Complexity

According to the participants, security roles were determined to be complex for a variety of reasons, including the demands of the operating environment, uncertainty when dealing with people and the changing threat environment. Such complexity suggests that while security practitioners may be operating within a relatively short time span of discretion, as uncovered in Phase One, the participants *felt* complexity results in higher-order decision making that may more closely align with higher strata positions (Clement & Clement, 2013). Whether this *felt* complexity is recognised by organisations is unknown, which may result in a lower structural seating than expected for the roles difficulty. However, an alternative view is that managing the complexity of individual people is still lower strata when compared to managing the complexity of a global operational environment for an organisation.

Nevertheless, security roles were found to be complex due to the substantial uncertainty found in working with people and trying to manage the risk of people-based problems from occurring that may impact an organisations future operating environment. For example, some participants noted that the security threat environment has changed dramatically over the last few years and continues to do so, requiring their department to be highly agile and capable of responding quickly. As one participant states "[the threat environment] is evolving on a daily basis and you know….incorporating cyber as a rapidly increasing risk to our operations and the global environment...[with] low sophistication terrorist incidents…absolutely the environments evolving faster now than ever." In large organisations, this means practitioners need to manage substantial internal relationships and balance business needs with security outcomes (Gill, Taylor, Bourne, & Keats, 2008).

Career Progression

Finally, results uncovered the security occupational stream had limited opportunity, in particular at more senior roles (Figure 2). Some of this restriction stems from the circumstance where senior security practitioners are applying generalist skills within a specialised work stream, but also due to the limited number of job opportunities.

Furthermore, several participants identified a lack of consistency in quality, education and experience of candidates, including the poor standards of training. For example, one senior level practitioner explains "one of the stresses we have are the people at the moment who we've inherited…we're stuck with the people who've exceeded their levels of incompetence." These elements of the security workforce could have substantial impacts on career progression opportunities. Nevertheless, some participants did identify opportunity, articulating the variety of skills needed in a security career. It is theorised that individuals starting in the security industry are exposed to a wide range of skills and are required to develop the capacity to deal with substantial uncertainty. If these individuals were to leave the security work strata and move into other areas of the business, they may have more opportunity to progress into higher order positions within the organisation than if they remained in the security function (Maitland & Sammartino, 2014; Speer, 2017).

Findings

In response to the research question: *To what extent, if any, does the Australian corporate environment have a career progression ceiling for security practitioners?* The hierarchical Corporate Security roles uncovered in Australian organisations suggests that there is indeed a career progression ceiling for Corporate Security. The discovered roles, as measured by the combined TCMT and WMS, comprise Stratum One (Operational), Two (Supervisory), Three (Managerial), and Four (General Managerial). These roles are oriented toward operational, professional and tactical tasks, with limited input into strategic activities. Individuals operating within an operational scope were very responsive to on-the-ground events and had limited forecasting abilities; however, they fulfilled an implementation, compliance and supervision tasking (Clement, 2015). The uncovered model of Corporate Security work is depicted below (Figure 2).

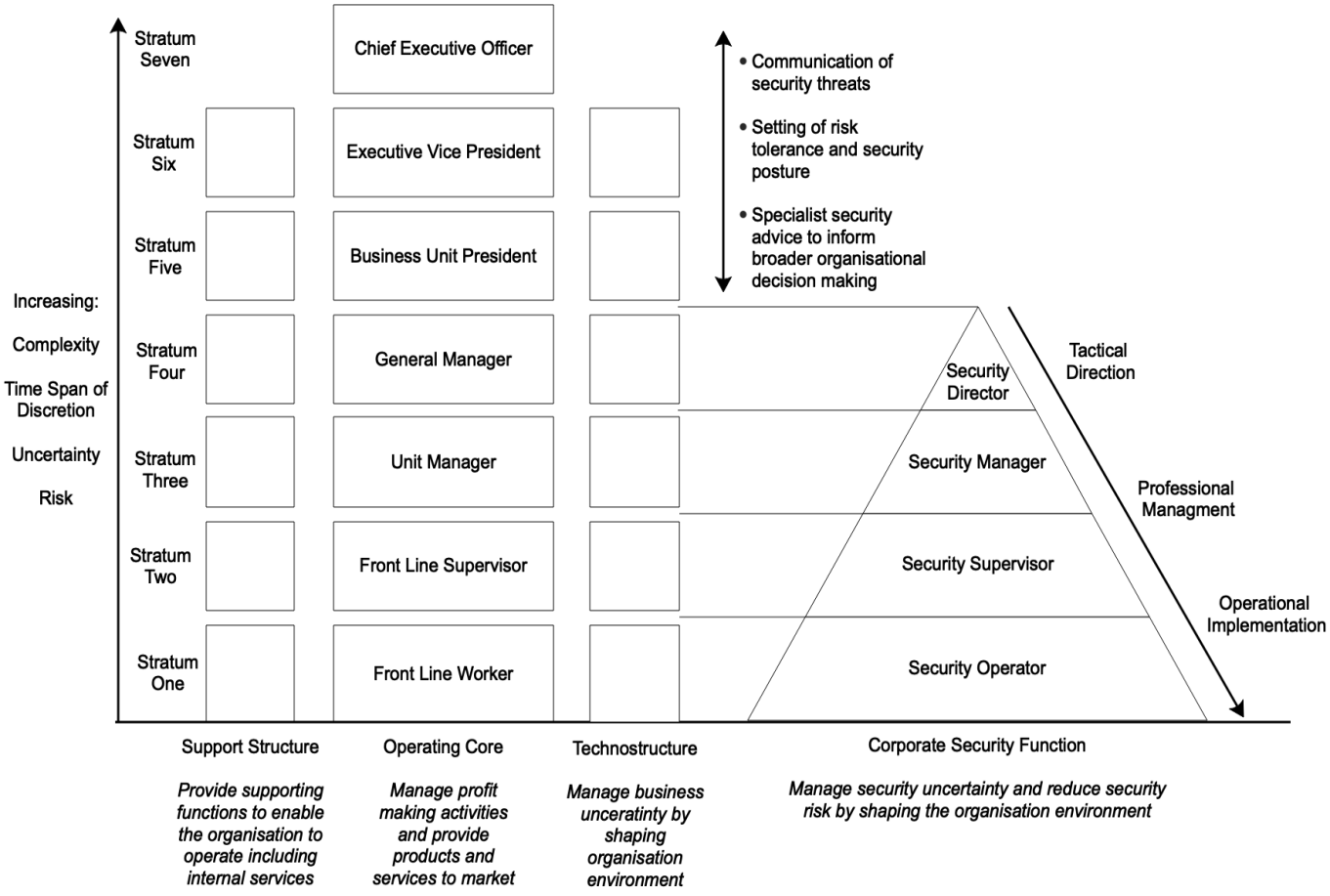

Figure 2. *The Uncovered Model of Corporate Security Work*

Subsequently, Corporate Security operates from a tactical position with its peak at the General Manager level, receiving overall direction from strategic executive decision makers. This model is supported by the socio-economic literature, where, for instance Papadakis and Barwise (2002) found that strategic decisions made at the executive level are long term and general. Strategic decisions guide tactical planning and operational implementation through an assessment of the overall operating environment, and the path needed to be taken to meet strategic business objectives. Thus, tactical planning and resourcing guides and supports the achievement of operational outcomes through the translation of the broad strategic direction through professional functions (Jaques, 1996).

In this model of Corporate Security (Figure 2), the risk tolerance is determined at the strategic level by executive decision makers with input from security specialists at the tactical level. Policies and procedures are developed to mitigate risk concordant with tolerance levels by Corporate Security (Somerson, 2009). Following, these policies and procedures are enacted and managed through professional roles; translating these into actionable items to be enforced by operational task outputs (Bamfield, 2014). As articulated below, this model is achieved through four levels of stratum work within the Corporate Security hierarchy.

Stratum One – Operational Security (Security Implementation)

Operational security roles were found to involve tasks such as rendering first aid, signing off reports, monitoring CCTV and managing incidents. For example, as one Stratum One participant described their role "99% of issues we get involved, if there's a fire alarm, we're the first responders, if there is a structural collapse, a floor, anything that has affected the centre, we as security will look after it as the first responder." Such an articulation of Stratum One security roles is consistent with the overarching security literature (Brislin, 2014; Nalla & Wakefield, 2014). Overall, individuals fulfilling operational taskings were implementing security strategy through concrete action and bounded decision making, with their direction and responsibilities defined by more senior positions within the organisation (Jaques, 1996). These tasks provide little opportunity to move beyond internal organisational structures as they fulfil a compliance function; nevertheless, there is some requirement to respond dynamically to emerging issues (Grobler, 2005; Nalla & Morash, 2002).

Stratum Two – Supervisory Security (Security Control)

Stratum Two Corporate Security roles were found to enact both professional and operational taskings. For example, some Stratum Two security workers were wholly bounded within operational work activities, working within defined procedures and responding to incidents (Clement & Clement, 2013). Others however, had a broader view, orienting their activities towards tasks such as directing staff, interpreting policy into actionable risk mitigation strategies, and synthesising disparate information streams into workable knowledge (Brooks & Corkill, 2014). A common theme for this stratum was the training of junior staff, supervising activities, managing departmental resources and maintaining deployed security control measures to support the broader risk management strategy.

Stratum Three – Specialist Managerial Security (Security Management)

Stratum Three roles are those that are responsible for the development of new systems and procedures, prescribing work to the lower strata of operations within the security function (Jacobs & Lewis, 1992) and managing the overall security risk and management of security controls for an asset or region. Such roles focus on solving internal problems with a specialist skill set; however, individuals at this level have begun to move to a more generalist management approach to problem solving (Brooks & Corkil, 2014; Jaques, 1996; Mumford et al., 2007). Subsequently, activities included managing staff to achieve various objectives across a time span of years, as well as complex environmental scanning, building relationships both internal and external, and overseeing contractual relationships. Typically, the Stratum Three roles were focussed on guiding the implementation of security risk management strategies. Receiving direction from higher order roles (Stratum Four), interpreting a direction, and then delegating responsibilities to the lower strata of work.

Stratum Four – General Managerial Security (Security Direction)

Stratum Four roles were found to require strong managerial skills and the ability to operate as a generalist within a specialist domain. Stratum Four roles were unable to set strategic direction, but were capable of influencing the

way strategic goals are determined and achieved at a tactical level (Maitland & Sammartino, 2014; Mumford et al., 2007). Subsequently, security activities carried out in Stratum Four roles required authority and influence to direct and shape the organisations risk exposure to security threats (Cubbage & Brooks, 2013). As one such Stratum Four participant explains, their role is to "get paid to exercise my judgement…I have career limiting conversations with important people in the organisation." Individuals had to demonstrate an understanding of the security function within the organisation and its purpose as whole, as opposed to specific sub-specialities within the discipline (Brooks & Corkill, 2014). While the role is broader, more complex, and functionally at the peak of the uncovered security function, individuals were still highly specialised and non-generalist in their view of organisational activities; aligning them strongly to technostructure roles (Jo, 2018).

With this in mind, the tactical tasks articulated by the participants align closely with the literature of general managerial roles (i.e. Strata Four/Five), and not higher order executive seatings that would be expected from their occupational title (Mintzberg, 2009). For instance, participants indicated some broader organisational skills such as implementing policy, making judgement calls, and setting strategic direction; however, it was always bounded within the Corporate Security domain. Moreover, where the individual managed several distinct business units, they were all security aligned areas of speciality. In other words, the uncovered peak security roles were not strategic in nature as they were restricted by their discipline speciality and problem-solving domain (Deming, 2013; Ivanov, 2015).

Overall, the uncovered security work hierarchy reinforces the security literature, that security is functionally significant within large corporate organisations, and plays a role in allowing business operations to function and be resilient in the face of security incidents (Coole et al., 2017; Cubbage & Brooks, 2013). Even so, findings support the socio-organisational literature to the incongruity of the security literature in the view of security not being strategically significant (Papadakis & Barwise, 2002). The findings support the concept of security being a partner in strategic decision making, but not an integral part of the final determination. The security function provides information and guidance, but the strategic direction is set by others that is then interpreted into a security strategy and directed by the security function.

Security Career Progression & Ceiling

In light of the uncovered Corporate Security work model, it is suggested that there is indeed a security occupational progression ceiling, in terms of both complexity as well as hierarchical progression (Freidman et al., 2015). This Corporate Security ceiling, as measured by Jaques (1996) work, was found to be Stratum Four (General Manager). Security roles, even at the strata peak, appear to be less complex than higher order executive positions due to the specialised and bounded focus of the work. Such a view is, in particular, due to the limited management of uncertainty outside the security domain (Maitland & Sammartino, 2014; Milliken, 1987). Moreover, in consideration of the discovered security roles along the work strata, the most senior security seatings align most closely with the socio-organisational literatures articulation of general managers and not executive managers (Clement, 2015; Clement & Clement, 2013; Mintzberg, 1980, 2009).

Subsequently, the study uncovered a security occupational ceiling at the Stratum Four level, accordant with the socio-organisational literature, equivalent to a General Manager position who undertakes tactical level work. While it is recognised that some security practitioners achieve role titles such as "Chief Security Officer" and such roles are supported by several academic and industry authors (ASIS International., 2004; Cubbage & Brooks, 2013), it is suggested that these role titles are not accurate descriptors of the actual tasking and activities undertaken when compared to the socio-organisational literature. Concordant with previous findings from Ludbey et al., (2018), the study found that the specialised nature of the Corporate Security function does not warrant a seat within the boardroom, and is more aligned to other specialised, technostructure roles, that feed specialised knowledge into broader business decision making undertaken by executive staff (Brickley et al., 2009; Sammarra et al., 2012).

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

Nevertheless, a career ceiling has been uncovered; however, a definitive understanding as to why such a ceiling exists is still limited. While it is likely the progression ceiling exists due to the specialised nature (technostructure) of individuals fulfilling security roles that do not directly create revenue, there are other influencing factors that should be further investigated. For example, the legislative operating environment appears to have an impact within the organisations. Does education and past-career background substantially affect security careers? These queries should be further investigated to better understand the nature of security careers, particularly at their peak hierarchical seating.

Conclusion

Corporate Security is a growing and significant industry and occupation in Australia, with increasing expectations to manage security uncertainty and risks to enable organisations to operate effectively (Smith & Brooks, 2012). In part, these expectations stem from corporate social responsibilities, as opposed to profit-making imperatives (Petersen, 2013). It is postulated that these growing expectations align with the modern interpretation of risk and the societal expectations around managing risk (Beck, 1992). Nevertheless, Corporate Security is responsible for identifying, assessing and managing potential security uncertainty and risks in support of the broader business strategies, directed by the executive strata (Coole et al., 2017; Ludbey et al., 2018).

The study found that Corporate Security operates within a technostructure, a group that provides a specialised role. Subsequently, Corporate Security needs to be responsive to emerging uncertainty and risks, and interpret the operating environment into actionable intelligence for executive decision makers. Such a role is specialised one and as such, influences opportunities for career progression (Strauss, 1975/2011). Furthermore, security has a

maximum career progression ceiling to stratum level four, being general manager. The aspiration for Corporate Security to be present at the higher stratum of organisational structures is understandable; however, specialisation, paired with the limited exposure to profit making activities, severely limits opportunity for progression and its overall impact at the strategic level (Speer, 2017). The study suggests that effective security functions should not seek to operate at the executive level, opposing the broader security literature; rather, concentrate on influencing and supporting executive decision making as a trusted advisor.

References

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

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

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

Barnes, B. (1995). *The Elements of Social Theory*. Princeton University Press. Retrieved from http://books.google.com/books?id=BPmXQgAACAAJ&pgis=1

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

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

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

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

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

Clement, S. D. (2015). Time-span and Time Compression: New Challenges Facing Contemporary Leaders *Journal of Leadership and Management, 2*(4), 35-40.

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

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

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). In C. University (Ed.). Columbia University.

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

Diefenbach, T., & Sillince, J., A.A. (2011). Formal and Informal Hierarchy in Different Types of Organization. *Organization Studies, 32*(11), 1515-1537.

Fay, J. J. (2002). *Contemporary Security Management* (1st ed.). Woburn, MA: Butterworth-Heinemann.

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

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

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

Füredi, F. (2006). *Culture of fear revisited: risk-taking and the morality of low expectation*. New York: Continuum.

Giddens, A. (1991). *Modernity and Self-Identity*. Cambridge: Polity Press.

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

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

Grobler, S. W. (2005). *Organisational Structure and Elliot 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?sequence=1 (3397-508-6)

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

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

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

Jaques, E. (1976). *A general theory of bureaucracy.* London: Heinemann Educational Books Ltd.

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

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

Jesus, B., Seibert, S. E., Kraimer, M., Wayne, S., & Liden, R. (2015). Measuring Career Orientations in the Era of the Boundaryless Career. *Journal of Career Assessment, 25*(10).

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

Koch, M., Forgues, B., & Monties, V. (2015). The Way to the Top: Career Patterns of Fortune 100 CEOs. *Human Resource Management, 52*(2), 267-285.

Krahmann, E. (2011). Beck and beyond: Selling security in the world risk society. *Review of International Studies*. https://doi.org/10.1017/S0260210510000264

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

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.

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

Ludbey, C., & Brooks, D. (2017). Stratum of Security Practice: Using Risk as a Measure in the Stratification of Security Works. *Security Journal, 30*(3), 686-702.

Ludbey, C., Brooks, D.J., & Coole, M. P. (2018). Corporate Security: Identifying and Understanding the Levels of Security Work in an Organisation. *Asian Journal of Criminology*, *13*(2), 109-128.

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

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

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *merican Journal of Sociology, 83*(2), 340-363.

Mintzberg, H. (1979). *The Structuring of Organizations*. Englewood Cliffs, NJ: Prentice-Hall Inc.

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

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.

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

Nalla, M., K.,, & Morash, M. (2002). Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions. *Security Journal, 15*(3), 7-19. doi:10.1057/palgrave.sj.8340119

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

Ocqueteau, F. (2012). Heads of Corporate Security in the Era of Global Security *Champ pénal/Penal field [En ligne], 8*. doi:10.4000/champpenal.8245

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

Papadakis, V. M., & Barwise, P. (2002). How Much do CEOs and Top Managers Matter in Strategic Decision-Making? *British Journal of Management, 31*(1), 83-95.

Petersen, K. L. (2014). The Politics of Corporate Security and the Translation of National Security. In Walby K. & L. R.K. (Eds.), *Corporate Security in the 21st Century. Crime Prevention and Security Management*. London: Palgrave Macmillan.

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

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

Rowbottom, R., & Billis, D. (1977). The Stratification of Work and Organizational Design. *Human Relations, 30*(1), 53-76.

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

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

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

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

Smith, C., & Brooks, D. J. (2012). *Security Science: The Theory and Practice of Security*. Oxford: Butterworth-Heinemann.

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

Stichweh, R. (2008). The Eigenstructures of World Society and the Regional Cultures of the World. In I. Rossi (Ed.), *Frontiers of Globalization Research* (pp. 133-151). New York: Springer.

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

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

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

Walby, K., Wilkinson, B., & Lippert, R. K. (2014). Legitimacy, professionalisation and expertise in public sector corporate security. *Policing and Society*. doi:10.1080/10439463.2014.912650

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

Willis, H. H. (2007). Guiding Resource Allocations Based on Terrorism Risk. *Risk Analysis, 27*(3), 597-606.

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