Original Article

# Stratum of security practice: Using risk as a measure in the stratification of security works

Codee R. Ludbey and David J. Brooks*
School of Computer and Security Science, Edith Cowan University, Joondalup 6027, Australia.

*Corresponding author.

**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.
*Security Journal* (2017) **30,** 686–702. doi:10.1057/sj.2015.50; published online 18 January 2016

**Keywords:** stratum; work; complexity; scanning; risk; corporate security

## Introduction

Organisations form the basis of governments, social structures, sport clubs, workplaces and all other forms of interaction in human life (Litterer, 1963). They are a vehicle for accomplishing goals and objectives through a system of interpersonal relationships aligned to a structure of authority, status and role (Robbins and Judge, 2012). Consequently, the structure of such organisations plays an essential role in the process through which goals are achieved. It is commonly accepted that this structure forms some level of hierarchy, which is considered to be the stratification of work (Mintzberg, 1980; Jaques, 1996, p. 36; Robbins and Judge, 2012).

The point of measure for this level of authority or work is discussed by Jaques (1964, 1972) as a role's discretionary time span. Mintzberg (1973, pp. 129–131) suggests that the level of authority within the hierarchy could be related to the types of roles fulfilled, for example, internal focus versus external focus. The true measure of work in a role is still a

contentious issue; however, all roles within an organisation must be accurately measurable for true efficacy. Owing to this one size fits all approach, the point of measure for work must be something that all levels of work are exposed to (Jaques, 1964; Ivanov, 2006).

Risk management, as a formal process, has emerged throughout private and public organisations (Power, 2007; Aven, 2008). Corporate security, embedded within these organisations, use risk management as a fundamental tool to mitigate its organisation's risks (Brooks, 2011). For example, within the Australian context most corporate security groups use Australian Standard ISO31000:2009 Risk Management and Australian Standard HB167:2004 Security Risk Management. Furthermore, risk is one such phenomenon where all levels of the work stratum are exposed (Smith and Brooks, 2013, p. 51). While there is no agreed definition of risk, it can generally be accepted that everyone is exposed to risk in one form or another (Sjoberg, 2000; Willis, 2007; Aven and Renn, 2009). Owing to risks all-encompassing nature within an organisation, risk can be used as a measure of work. Therefore, given the robust focus corporate security has on risk management, risk became the study's stratum measure of security works.

The article explored organisational risk, its relationship to task complexity and the use of risk as a measure of work stratification within an organisation's security context. Consequently, exploring the research question: *Within Corporate Security, can risk measure work stratification?*

## Background

Security, and in particular, corporate security, is a developing academic discipline that is immersed in the management of risk (Smith and Brooks, 2013, pp. 51–79). This discipline is a practice domain that provides for the protection of people, information and assets within an organisation, existing to provide self-protection of the corporation. Furthermore, corporate security allows for the executive team to exercise control and governance across the organisation in the face of threats (Brooks and Corkill, 2014). Nevertheless, as a practising domain, corporate security undertakes a broad range of activities across multiple agencies with differing structures (Gill, 2014, p. 1); therefore, corporate security requires better understanding of its undefined boundaries and structure. Owing to the nature of an effective corporate security function and its requirement to operate throughout the hierarchy of the organisation, the ability to accurately measure, define and understand the corporate security stratum of occupational work is important for educational institutions, professional bodies and industry practitioners (Jaques, 1972; Mintzberg, 1980; Brooks and Corkill, 2014). In part, this study begins to address some of these issues.

Over the past three decades, risk management has become a formal discipline that has emerged throughout private and public organisations. The practice of risk management is well-established, with its own body of knowledge, national standards and domain practitioners (Brooks, 2011, pp. 17–18). Risk management is a common undertaking supported by tools or processes for many managers within a corporation. Such use is extensive within corporate security, where threat is considered a driver in security risk within the corporate function.

The measurement of role seniority through task comparison is not a new concept (Jaques, 1951; Laner *et al*, 1969). Many organisations use some form of work measurement, usually

within the context of employee performance reviews to manage and develop staff over time (Robbins and Judge, 2012). Such tools vary in scope and functionality, with some being more successful than others (Laner *et al*, 1969). However, many tools do not have appropriate scalability across an entire organisation, with some measuring lower-level roles well, but breaking down at higher levels of work and *vice versa* (Laner *et al*, 1969; Ivanov, 2006, 2011).

## Significance

The role and function of corporate security in the literature continues to be undefined outside of contextual definitions. Corporate security is embedded into most public and private medium to large organisations to drive corporate control and responsibilization (Brooks and Corkill, 2014). However, the group lacks a defined body of knowledge, differing language of security concepts, clear entry routes and career paths, and continues to struggle with undefined training and educational pre-requisites and standards, with restricted scholarly attention. Such factors lead to a restricted understanding of what skills and knowledge corporate security practitioners require in their day-to-day activities. Owing to these issues, the practice area of corporate security cannot be considered a profession (Brooks, 2013; Coole and Brooks, 2015). Nevertheless, the group is significant in providing security across the broad spectrum of both government and private organisations including national critical infrastructure.

Corporate security is a discrete sector of the larger security domain (Brooks and Corkill, 2014). For example, Sarre and Prenzler (2005) articulate the delineation of private and corporate security. They state that private security is associated with the provision of contract services, whereas corporate security is associated with in-house services. Such work boundary is further depicted by Sarre and Prenzler (2005) through juxtaposition with policing roles, where security is a prevention mechanism, and policing is an enforcement one (Fischer *et al*, 2008).

As a prevention function, corporate security is embedded in the structure of an organisation and is responsible for engaging with security risk on behalf of the business (Talbot and Jakeman, 2009; Cubbage and Brooks, 2013). By leveraging this risk exposure and grounding itself in the broader socio-organisational literature, this study undertook a novel and objective approach in the investigation of security work. This approach allowed an external examination of the corporate security function conducted with an appreciation of organisational goals, objectives and structure, which was not inherently biased to potential misconceptions from the security literature. Such an approach enabled an investigation of the occupational stratum of work in the corporate security function; articulating work roles and positioning the function within the broader organisation.

## Theoretical Framework

The literature informing this study stem from socio-organisational theories of work that continue to be developed in recent times (Craddock, 2002; Kalser *et al*, 2011). Through consideration of the genesis of these socio-organisational theories, an informed and robust argument can be made through their application. The study drew from the task complexity,

information scanning and requisite organisation literature in the investigation of security works.

## Task complexity

A task can be defined as 'a discrete unit of work with target completion time and quality standards, either given by a manager to a subordinate explicitly or implicitly, or generated by a general responsibility' (Jaques, 1964, p. 13). More broadly, task structure consists of characteristics of a task to be accomplished. Such structure includes component complexity, component organisation and component redundancy. Simply, component complexity can be defined in terms of information processing and/or memory storage requirements (Wood, 1986; Campbell, 1988; Haerem and Rau, 2007). Component organisation refers to similar demands of different task components because of their interrelationship to the overall task. Finally, component redundancy refers to the degree of overlap existing among each task component (Naylor and Dickinson, 1969; Haerem and Rau, 2007).

Jaques (1964, p. 23) developed a scale of task complexity that enables measurement through the discovery of the 'longest period which can elapse in a role before the manager can be sure that his subordinate has not been exercising marginally sub-standard discretion continuously in balancing the pace and quality of his work'. This time span of discretion in a role is a method of measuring task complexity and by extension, levels of work. Such levels of work within a role have been critically reviewed by the literature, with significant supporting evidence being uncovered (Craddock, 2002). Ivanov (2006) has shown that using the time span of discretion measurement is a viable tool for measuring an individual's positioning on the stratum of work, but has noted the tool has difficulty aligning workers at the lower strata of organisations.

## Information scanning

The work of a manager is information driven (Mintzberg, 1973, p. 4; Robbins and Judge, 2012). Therefore, day-to-day decisions and long-term planning are reliant on robust information feeds (Mintzberg, 1973). Scanning is a type of information seeking behaviour that is externally directed in aid of understanding events and trends that are relevant to the organisation (Case, 2002, pp. 248–249; Robson and Robinson, 2013). This behaviour is often referred to as environmental scanning in the business context. Scanning includes both general information collection and purposeful searching for specific information to guide managerial decision making (Case, 2002). Supported as a necessary business process, Auster and Choo (1994a) indicated that there is a positive correlation between perceived uncertainty and the amount of scanning conducted, and this finding is supported by the broader socio-organisational literature (Robbins and Judge, 2012).

## Requisite organisation

Jaques (2002) suggests that the stratification of an organisational structure is a reflection of the stratification of human capability to carry out work. Consequently, through the

measurement of task time span, it is possible to identify a hierarchical strata of work, with each level in the hierarchy increasing in task complexity (Craddock, 2002). Significantly, human capability is a measure of the capacity to work under greater uncertainty, tension and anxiety (Jaques, 2002). Such stratification can further be explained as structured, defined tasks at the bottom, and unstructured, ill-defined tasks at the top (Mintzberg, 1973, p. 15, 1980; Ivanov, 2011). Jaques (1996) identified seven such roles of complexity within an organisation, those being: front-line work, first-line manager, unit manager, general manager, business unit president, vice president and chief executive officer.

## Methodology

The study consisted of two parts; the first comprised of a literature review and the second, an online survey. The literature review was framed in the broader sociological theory of structural functionalism. Furthermore, the review was conducted to orient and ground the study (Creswell, 2007, 2009), and its outcomes were used in the development of the survey instrument and embedded work measurement scale (WMS) tool.

The second part of the study used an anonymous online survey, which consisted of two instruments with a total of 19 questions. The surveys were distributed purposively to participants through email and social media, using professional networks within Australia and the United Kingdom. Consequently, the sample consisted of individuals who were currently working in the security industry within Australia and the United Kingdom, were over the age of 18, and held any level of experience or education. These participants were specifically targeted to ensure responses aligned across varying levels of the work stratum. Consideration was given to participants' work place, job title, level of experience and professional networks to ensure a spread of responses across the stratum (Creswell, 2009). These participants were asked to forward the survey onto their peers for further data collection, ensuring further penetration of each strata of work. Random sampling was a consideration for the research, however, to ensure effective penetration of the varying strata of work, it was considered to be an ineffective approach.

Internet survey response numbers can be as low as 10 per cent (Fowler, 2014), and as such Cohen *et al* (2007, p. 286) stress the importance of wide and continual distribution. Owing to time constraints this continous distribution was not feasible; therefore, approximately 30 participants were selected for survey distribution with a response number of 14 achieved. Accordingly, the survey achieved response number of 47 per cent, which was in excess of expectations, and aligns with the purposive approach taken for the research. Nevertheless, the limited sample does have significant implications to the application of this study's findings to the broader corporate security population. However, a small sample can be indicative of the feasibility of this novel approach to the research.

The online survey asked participants their current job title, how many employees they managed, and where and how they seek risk information. Risk information source options included customers, government sources, business associates, newspapers, internet, manager, email, internal staff, policy and procedures (Auster and Choo, 1993, 1994a, b; Case, 2002; Robson and Robinson, 2013). These questions allowed a degree of validation of the participants' work stratum level. In addition, two measurement tools were included to

provide a level of inter-method triangulation, as well as to support construct and content validity (Denzin, 1989; Creswell, 2007, 2009).

The first instrument, the WMS, examined participants' current level of work through their longest risk task or tasks conducted into the future. The WMS was designed through examination of the literature (Mintzberg, 1973, 1980; Robbins and Judge, 2012), but primarilly being aligned to Jaques' (1996) time span of discretion measure. Consequently, the WMS was designed to explore many aspects of an individual's risk exposure in their role. Such exposure was examined through asking the participants a series of questions about different risk related aspects of their work and sought how far into the future they conduct these aspects of work. Groupings of time span across multiple tasks were an indicator for each individual's level of work. This process was conducted because of the limitations of an online survey, as Jaques' (1996) initial work suggests that an individual's level of work cannot accurately be identified through self-assessment; however, this limitation was mitigated through cross-check measures.

The second instrument, the Task Complexity Measurement Tool (TCMT), provided a measure of task complexity of an individual's work role. This measurement was achieved through a Likert scale, with a series of questions about the conduct of work in regards to risk. The TCMT instrument repeated, in content, a tool used by Jaques (1996) in the assessment of task complexity.

The study's instruments reliability and validity were achieved through content, construct and face validity (Creswell, 2007, 2009). The instruments were designed to ensure there was a direct correlation to the literature. Furthermore, the instruments were further judged by two security academics with suggestions to improve the tools and reflect the aims of the study. Finally, the use of both the WMS and TCMT instruments ensured a level of research triangulation, improving the reliability of the results through correlation (Denzin, 1989) and with past validity.

## Analysis

Data were analysed, with the WMS and TCMT evaluated to provide an 'assessed level of work' (Table 1). The data collected relating to the job title, job level, number of employees and information source were used as a cross-check measure for the final assessed level of work.

The analysis indicated that 15.4 per cent of respondents were assessed as Stratum I, 30.8 per cent assessed as Stratum II, 23.1 per cent assessed as Stratum III, 23.1 per cent assessed as Stratum IV and 7.8 per cent assessed as Stratum V. The assessed level of work was conducted in-line with the methodology and relied on cross-check measures to ensure reliability. As 77 per cent of respondents in the TCMT response were recorded as higher than their final assessed level of work, it was reasonable to assume that the TCMT was not a reliable measurement instrument in this study. Consequently, the WMS was used in conjunction with the cross-check measures such as job title, number of employees managed and information sources used to assess the level of work.

The participant's use of information in their role appears to be both internally and externally directed no matter the assessed stratum of work in the role. The use of the scanning literature in the construction of the survey instrument may have to be adjusted in further studies to ensure a more accurate measure.

**Table 1:** Survey data, with assessed levels of work

| *Job title* | *Job level* | *Number of employees* | *Information source* | *WMS result* | *TCMT result* | *Assessed level of work* |
|---|---|---|---|---|---|---|
| Not assessed | I | 0 | Staff, Manager | I | VII | I |
| Electronic security installer | I | 1 | Customers, Government, News, Trade, Emails, Procedures, Internet | I | I | I |
| Domestic security advisor | II | Not assessed | Customers, Associates, Government, Staff, Emails, Procedures, Manager | II | VI | II |
| Assistant director | II | 2 | Customers, Associates, Government, News, Trade, Internal Staff, Procedures, Manager, Internet | II | IV | II |
| Business owner | II | 3 | Associates, Emails, Internet | II | VI | II |
| Community safety coordinator | II | 3 | Customers, Associates, Government, News, Staff, Emails, Procedures, Manager, Internet | III | II | II |
| Not assessed | III | 9 | Government, News, Trade, Procedures, Internet | III | VI | III |
| Security manager | III | 20 | Customers, Associates, Government, News, Trade, Staff, Emails, Procedures, Manager, Internet | III | VI | III |
| Security project manager | III | 3 | Customers, Associates, News, Staff, Emails, Manager, Internet | III | V | III |
| Regional business unit manager | IV | 40 | Customers, Associates, Government, News, Trade, Staff, Emails, Procedures, Manager, Internet | IV | II | IV |
| Security consultant | II | 500+ | Associates, Government, News, Staff, Procedures | IV | VII | IV |
| Senior risk manager | IV | 4 | Internet | IV | VI | IV |
| Not assessed | IV | 205 | Customers, Associates, Government, News, Staff, Emails, Procedures, Manager, Internet | V | VI | V |


 

## Risk as Measure of Work Stratification

Risk is an underlying component of day-to-day life and whether it is acted upon consciously or unconsciously, everyone practices some form of risk management (Smith and Brooks, 2013, p. 51). According to Aven and Renn (2009), risk can be defined as 'uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value' (p. 1). Consequently, an exploration of Jaques' requisite organisation is discussed in aid of determining the feasibility of using risk as a point of measure for task complexity.

Tasks differ in their predictability and thus, the uncertainty that must be dealt with during their execution (Tushman and Nadler, 1978). The amount of uncertainty in a task is related to the information processing capability to cope with the task (Tushman and Nadler, 1978; Jaques, 1986). Furthermore, the environment in which a task needs to be completed impacts the complexity of the task. The task environment consists of external factors that introduce uncertainty into the task. The more dynamic the task environment, the more complex and uncertain the task is to complete.

The study posed the research question: *Within Corporate Security, can risk measure work stratification?* The question is addressed in the context of risk, information seeking behaviour to risk, and the alignment between risk and the work stratum.

### Risk context

Risk can be seen as the uncertainty surrounding the events, consequences, or outcome of an activity (or task). Within an organisation, it is prudent to consider the ability to manage risk as a measure of an individual's capacity for coping with rising complexity (Tushman and Nadler, 1978; Jaques, 1996; Aven and Renn, 2009). If we examine the changing nature of risk in terms of context definition, the differences in complexity become apparent. For example, an individual dealing with personal risk has a defined context within which to identify and respond. Juxtaposed to this, a general manager is concerned with risks to the broader business unit that has a larger and less defined scope for risk identification. Jaques' strata place significant emphasis on 'projecting' tasks across time, consequently risk was aligned to strata based on 'projection'.

In this study, such a relationship was immediately apparent. Through examination of the individual responses, the differing approaches to risk can be seen. Stratum I individuals, for example, only consider risk from a very short-term perspective (days to months) and do not indicate perception or appreciation for long-term risks and consequences. Juxtaposed to Stratum I, Stratum V individuals appear to consider long-term risk developments and potential long-term consequences (5–10 years). Further examination of the data indicates a progression along the stratum, with each level of work showing individuals with different risk perceptions. Although the analysis did indicate cases where a Stratum II individual considered long-term risks (1–5 years), for example, other areas of risk perception such as vulnerability assessments and consequence assessments were considerably shorter term.

### Information seeking behaviour when exposed to risk

Another example of an increase in complexity is the use of scanning in information seeking behaviour (Case, 2002). The work conducted by Auster and Choo (1994a) has shown that

the more uncertain the operating environment, the more an individual will focus on external information feeds. The inverse of this is where the task is more prescribed, the more an individual will seek information internal to the organisation (Mintzberg, 1973, pp. 13–15; Case, 2002; Robins and Judge, 2010).

Examination of the data provided a contrary viewpoint to the literature, indicating that individuals do not seek different information depending on their level of work. Consequently, the analysis indicates that some Stratum I individuals seek information from similar sources to their managerial counterparts in Stratum II through V. Such a result could be indicative of poor survey question structure or possibly the changing nature of information gathering because of the increasingly ubiquitous availability of information, and information technology access. Further exploration of this outcome is necessary, as the restricted study sample size could be a contributing factor.

## Risk exposure and levels of work in the security industry

Jaques (1996, 2002) argues that the increase in complexity of a role is because of the increase in the time it takes for the longest assigned task to be completed. Furthermore, complexity can be considered in the terms of the number of variables that have to be dealt with, their tendency to change and their readiness to be identified (Jaques, 1996, p. 64). Such a view can be held against different roles within the corporate security domain. As put forward by Griffiths *et al* (2010), the corporate security manager has a number of knowledge categories through which work is completed. Brooks and Corkill (2014) further discuss the implementation of these knowledge categories across an organisation, with knowledge use becoming more complex as categories begin to interrelate with strategic organisational direction.

At the lower end of the stratum, tasks are more defined, technical knowledge is more important in completing tasks, and risk is more operational (Mintzberg, 1973; Jaques, 2002; Brooks and Corkill, 2014). Front-line security management focuses on direct control of the internal workforce and interacts with a restricted external workforce (Brooks and Corkill, 2014). Furthermore, front-line security management staff are generally directly responsible for site security and management of a specific facility (Brooks and Corkill, 2014). It is suggested that Stratum I and Stratum II workers have a very direct engagement with risk, considering immediate and readily identifiable threats. Such a view is supported by other authors (Fischer *et al*, 2008, p. 148; Garcia, 2008, pp. 25–41).

At the middle level, responsibilities shift to managing the security business unit, and risk focus shifts from an operational outlook to a tactical and external one (Jaques, 1996; Brooks and Corkill, 2014). Engagement with risk at this level begins to shift externally; however, it is still directed within the business and not the overarching organisation's strategic vision (Jaques, 1996, p. 69). Such a focus suggests that dealing with risk and uncertainty at this level is, as discussed by Mintzberg (1973, pp. 13–14), unstructured or 'un-programmed' and the manager cannot use a pre-defined method to mitigate or manage the risk. Significantly, this is supported by the literature (Sennewald, 2011).

At the upper echelons of the corporate stratum, security managers move towards a governance role (Talbot and Jakeman, 2009; Brooks and Corkill, 2014). This role requires direct engagement with extensive risk and uncertainty that is consistently variable and hard to identify (Jaques, 1996, pp. 70–71). Interestingly, the data collected did not indicate any

individuals operating at this level of work. While the restricted sample size could account for this, consideration must be given to the broader socio-organisational literature. This body of work suggests that security is restricted within the business unit, with little capability to influence long-term decision making and strategic direction (Fayol, 1949; Mintzberg, 1980; Robbins and Judge, 2012). Such restriction is because of the specialist nature of the corporate security function, where higher strata work is generalist in nature with no specialist application.

In addition, the analysis suggests that the maximum level of work in the corporate security function is indeed Stratum V; suggesting that there is some 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 occupational activities of work in organisations. For example, Mintzberg (1973) alongside Jaques (1996) and Robbins and Judge (2012) postulate that higher strata work requires a generalist managerial approach, with limited specialist skills. 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.

Thus, the study indicates that as risk exposure along the work hierarchy develops from explicit to implicit risk, so does the underlying complexity of the role to manage the risk. This relationship provides a level of measurement for task complexity, and, according to Jaques (1996) the ability to align individuals along the stratum of work in the corporate security domain.

## Security as a tactical enabler of business operation

Talbot and Jakeman (2009) and Cubbage and Brooks (2013) articulate that security decision making should ultimately be made within the executive levels of work of an organisation. They argue that a Chief Security Officer should be responsible for all security related issues across an organisation to ensure the security function is value adding and supporting long-term business objectives. Nevertheless, the confinement of the corporate security function within the business unit supports the discussion presented by Brooks and Coole (2011), who posit that the security practitioner does not have the opportunity to contribute directly to the executive level of work because of misunderstanding and misperception of the function itself by executive management.

It is suggested that the corporate security function is focussed on tactical and operational level tasks and responsibilities, with many security management texts taking this approach (Fay, 2002; Sennewald, 2011). Furthermore, Fayol (1949) articulated that security must be embedded throughout an organisation to ensure efficacy in its operation; however, it does not operate in an entirely specialised form at the executive level. Stemming from this discussion, Mintzberg (1980) outlines the concept of the ‘technostructure’ which is a supporting technical function that provides analytic techniques for the design and maintenance of an organisations’ business functions in aid of ensuring adaption to operational and environmental concerns. Jaques (1996, p. 44) supports this notion and elaborates by explaining that specialist support staff operate alongside mainstream operational functions assisting core business functions in their work.

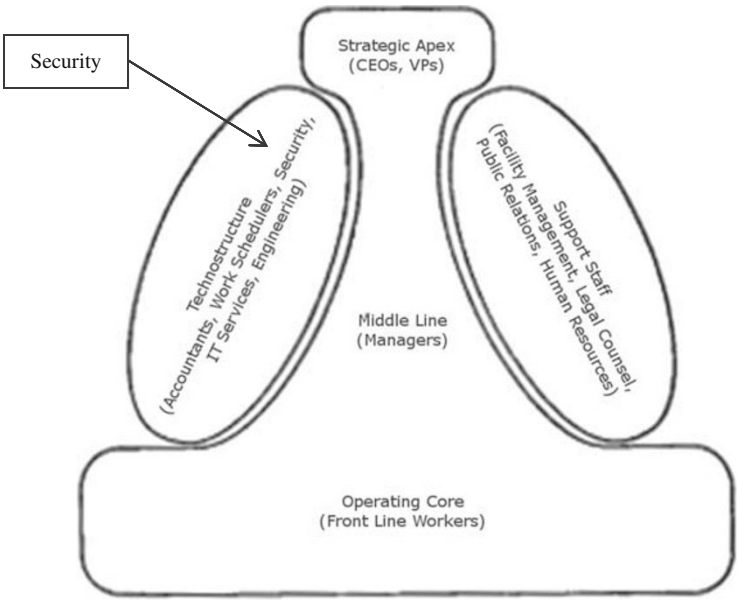


**Figure 1:** Organisational structure with security as a supporting function in the technostructure.
*Source*: Adapted from Martin and Fellenz (2010).

The study indicates, through an alignment of the broader socio-organisational and corporate security literature, that security operates within the technostructure and is a supporting 'business enabling' function. For example, Figure 1 identifies a number of common functions within organisations and maps security accordingly. Furthermore, the analysis provides supporting evidence to suggest that the nature of security is to operate within a tactical world view, with no evidence to suggest strategic operations. In addition, it is argued that while security will never provide robust revenue streams, it will ensure business continuity, the protection of other business unit revenue streams and the assurance of a secure work place (Fischer *et al*, 2008; Talbot and Jakeman, 2009; Smith and Brooks, 2013).

## Findings

Brooks and Corkill (2014) articulate a skill progression where an individual requires more general managerial skills and less technical skills as they progress up the hierarchy of work, such a view provides a starting point for considering each level of identified work in more detail. This articulated skill progression is generally agreed upon in the broader socio-organisational literature (Robbins and Judge, 2012). Significantly, the five distinct strata of work identified by the findings indicate that almost half of security work is conducted within an operational time horizon of 1 day to 1 year. Analysis correlates this operational level of work with Stratum I and Stratum II roles, comprising of direct and visible problems, and restricted and highly specialist work environments (Mintzberg, 1973; Jaques, 1996). Tactical time horizons are encountered at Stratum III and Stratum IV, between 1 and 5 years.

**Table 2:** Corporate security role alignment

| *Stratum* | *Role title* | *Function descriptor* | *Role type* |
|---|---|---|---|
| I | Security Guard, Security Technician, Investigator, Security Consultant | Work is service oriented, and focussed on operational risk that can be overcome or mitigated through direct trial and error approaches to security control, and problems can be solved with technical knowledge and pre-learned behaviours and tools | *Operational* 1 day–1 year |
| II | 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 immediate and readily identifiable risks | |
| III | Security Manager (Services, Risk, Operations) | Work requires strong diagnostic skills to solve security problems. Individuals must consider a situation using their technical security knowledge and interaction with internal and external stakeholders to develop short-term mitigation strategies while considering consequences | *Tactical* 1 year–5 years |
| IV | Senior Security Manager (Risk, Investigations, Emergency) | 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 | |
| V | Security Director | Work requires extensive engagement with external and internal risk with an implied understanding of the extensive interaction between business operations and the operating environment. Individuals at this level plan security engagement with risk and provide tactical planning for security risk mitigation on behalf of the organisation. The work conducted at this level must have a strong appreciation for the security function, but is a business manager first, and a security specialist second | |
| VI | NA (within security) | NA | *Strategic* 5 years–20+ years |
| VII | NA (within security) | NA | |

*Source*: Adapted from Mintzberg (1980); Jaques (1996); Sennewald (2011); Brooks and Corkill (2014).

These levels of work involve progressively more abstract thinking, stakeholder engagement and managerial skills. The strata identified comprise the lower portion of the broader occupational stratum of work in organisations, indicating corporate security's functional boundaries as a subset of this whole (Table 2).

The study has indicated that within the context of corporate security, there is a relationship between risk and uncertainty in work level. In addition, it suggests that security is at a lower work task stratum than a practitioners' title may suggest. Such findings allow us to better understand how security aligns within the greater corporate structure, within both a

work task perspective and in stratum levels. Understanding work tasks within the corporate stratum allows security to benchmark against their allied practitioners, gaining a greater insight into the roles of corporate security. It is considered that security is a tactical enabler to strategic business function, therefore can never, or should never be, at a higher stratum of work.

Consequently, the implications of these findings are extensive. Education can use this understanding to better tailor risk discussion to the level of work being taught. For example, guard training should consider direct risk engagement; whereas, managerial roles need to consider more complex and long-term risk exposure from an external context. Security practitioners may also better map and progress their careers and align this progression to other areas within an organisation.

Furthermore, better understanding of the security function and its functional alignment and seating within the broader occupational stratum of work allows for progression of the professionalisation of the function. In addition to this, by understanding the occupation and its place within the broader managerial strata, organisations can shift their structure to better harness security functions outputs and maximise its effectiveness in enabling business operations.

Finally, articulation of the corporate security work stratum could provide government with a better understanding of risk exposure and its changes along the security stratum of work, providing context for policy development and industry engagement.

## Further Research

There is a relationship between risk and uncertainty in work, which is highlighted through applied context such as security and the literature surrounding information scanning (Mintzberg, 1973; Jaques, 2002; Brooks and Corkill, 2014). Such a relationship is to date unexplored in any detail; however, it may yield insights into the measurement of work within a role. It is suggested that further research could be conducted to investigate the relationship between risk and the measured level of work complexity. Therefore, the following areas merit further research:

1. Measuring perceived risk and uncertainty at each level of Jaques' (1996, 2002) strata of work.
2. Measuring the knowledge categories identified by Brooks (2013) against Jaques' strata of work.
3. Further investigation of the scanning literature and its relationship to Jaques' body of work.
4. Case study analysis of the seating of corporate security within organisations using Jaques' (1972) strata of work.

If these areas can be further explored and compared the true nature of this relationship can be discovered. Nevertheless, it may also be prudent to explore this relationship through another measure other than scanning, such as stress or anxiety coping methods with increased uncertainty (risk) to ensure robustness of the identified relationship.

Finally, the validity of Jaques' stratum of work in today's corporate environment could be further tested. It can be argued that few, if any, Stratum VI and Stratum VII managers operate

with such a time span of a decade or longer in today's dynamic environment. Furthermore, it is possible that discretionary time span across the stratum has reduced; due in part, to the speed that business now operates at with information technology, data access and the like.

## Limitations

The study had a number of limitations, which must be addressed when considering the analysis and discussion. First, the limited sample size of this study has the potential to skew the analysis and provide false insights into stratum of work within the security industry. Furthermore, Boal and Whitehead (1992) suggest that Jaques' underlying theory is not robust enough to be applied to all situations. They suggest that cognitive capacity must be considered in conjunction with behavioural traits. Boal and Whitehead (1992) further suggest that Jaques' work is only relevant in measuring those who deal with 'tame' problems, and it could be argued that corporate security practitioners are exposed to, and manage 'wicked' problems. Ivanov (2011) discusses Jaques' theory in regards to modern organisations and suggests that they operate at a highly compressed level of work. Consequently, the identified time horizons in modern work environments need to be considered, as the changing pace of work may have an impact. This discussion could indicate that Jaques' theory requires further development in consideration of modern technology and work flows, especially when considering the de-layering of organisations with the adoption of such technology. This de-layering may also affect the identified risk exposure along the work stratum, and as such further research is advised.

## Conclusion

Corporate security is an embedded function within most organisations; however, there is a restricted understanding in how this function aligns in hierarchy and influence within its corporation. Jaques (1996) identified an underlying stratification or hierarchy of work across all organisations that can be measured through an individual's time span of discretion and an individual's capability to cope with complexity (Mintzberg, 1973; Craddock, 2002). In the information seeking literature, the concept of scanning has also substantiated Jaques claim partially through identifying that higher-level managers deal with more uncertainty than lower-level managers, and thus cast a broader net for information than their lower-level counterparts (Case, 2002). In consideration of the corporate security domain, such stratification of work has not been identified or measured, with unclear career progression, lack of role consistency and undefined function.

Through the use of the Jaques requisite organisation, a survey was distributed to corporate security practitioners across the stratum of security work. Participants were purposively selected and asked to provide a snowball sample for data collection. Respondents were questioned about their work in relation to risk exposure and management, with the intent of identifying a relationship between risk and the level of work in a role.

The study supported the claim that risk is inherently tied to task complexity and the level of work conducted in a role. Within the context of corporate security, there is a relationship between risk and uncertainty in work level. Findings suggest that as a security practitioner

progresses upwards in the corporate stratum, their risk context broadens externally to include more variability and uncertainty in terms of threat. This change in context directly impacts the level of complexity in the role. Furthermore, it is suggested that at the higher levels of corporate security the practitioner is at a lower work task stratum than their title suggest. For example, a security director may be undertaking a task complexity one or two levels below what their title suggests. Evidence from this discussion indicates that security is a tactical function that will not enter the executive stratum, as it is merely a business enabler with the technostructure to support the organisation.

Understanding the corporate security stratum allows a better alignment of security to the greater corporate structure, allied practitioners and actual roles. Such understanding benefits corporate security in moving towards a professional practice area, within clear and bounded roles and skills.

## References


Auster, E. and Choo, C.W. (1993) Environmental scanning by CEOs in two Canadian industries. *Journal of the American Society for Information Science* 44(4): 194–203.

Auster, E. and Choo, C.W. (1994a) CEOs, information, and decision-making: Scanning the environment for strategic advantage. *Library Trends* 43(2): 206–225.

Auster, E. and Choo, C.W. (1994b) How senior managers acquire and use information in environmental scanning. *Information Processing & Management* 30(5): 607–618.

Aven, T. (2008) *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities*. Chichester, UK: John Wiley & Sons.

Aven, T. and Renn, O. (2009) On risk defined as an event where the outcome is uncertain. *Journal of Risk Research* 12(1): 1–11.

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

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

Brooks, D. and Corkill, J. (2014) Corporate security and the stratum of security management. In: K. Walby and R. Lippert (eds.) *Corporate Security in the 21st Century: Theory and Practice in International Perspective*. 1st edn. Palgrave Macmillan, pp. 216–234.

Brooks, D. and Coole, M. (2011) Mapping the organizational 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, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=asi, accessed 7 January 2016.

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

Campbell, D.J. (1988) Task complexity: A review and analysis. *Academy of Management. The Academy of Management Review* 13(1): 40–52.

Case, D.O. (2002) *Looking for Information A Survey of Research on Information Seeking, Needs, and Behavior*. San Diego, CA: Elsevier Science.

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

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

Craddock, K. (2002) *Requisite Organization Annotated Bibliography: An Annotated Research Bibliography on Elliott Jaques*. 6th edn. Global Organization Design Society, http://globalro.org/index.php/go-library-3/comprehensive-annotated-ro-bibliography , accessed 7 January 2016.

Creswell, J. (2007) *Qualitative Inquiry & Research Design Choosing Among Five Approaches*. 2nd edn. Thousand Oaks, CA: SAGE Publications.

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

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

Denzin, N.K. (1989) *The Research Act: A Theoretical Introduction to Sociological Methods*. 3rd edn. Englewood Cliffs, NJ: Prentice-Hall.

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

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

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

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

Garcia, M.L. (2008) *The Design and Evaluation of Physical Protection Systems*. 2nd edn. Sydney, New South Wales: Butterworth-Heinemann.

Gill, M. (ed.) (2014) *The Handbook of Security*. 2nd edn. New York: Palgrave Macmillan.

Griffiths, M., Brooks, D. and 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, http://igneous.scis.ecu.edu.au/proceedings/2010/secintel/griffiths.pdf.

Haerem, T. and Rau, D. (2007) The influence of degree of expertise and objective task complexity on perceived task complexity and performance. *The Journal of Applied Psychology* 92(5): 1320–1331.

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, 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): 94–110.

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

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 edn. London: Heinemann Educational Books.

Jaques, E. (1972) *Measurement of Responsibility A Study of Work, Payment, and Individual Capacity*. New York: John Wiley & Sons.

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

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 edn. Arlington, VA: Carson Hall and Co Publishers.

Jaques, E. (2002) The psychological foundations of managerial systems a general systems approach to consulting psychology. Paper presented at the Midwinter Conference of the Society of Consulting Psychology, San Antonio, TX.

Kalser, R.B., Bartholomew, C.S., Overfield, D.V. and Yarborough, P. (2011) Differences in managerial jobs at the bottom, middle, and top: A review of empirical research. *The Psychologist-Manager Journal* 14(2): 76–91.

Laner, S., Crossman, E.R.F.W. and Baker, H.T. (1969) *Measurement of Responsibility: A Critical Evaluation of Level of Work Measurement by Time-Span of Discretion*. Berkeley, CA: California University.

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

Martin, J. and Fellenz, M. (2010) *Organizational Behaviour & Management*. 4th edn. Hampshire, UK: Cengage Learning EMEA.

Mintzberg, H. (1973) *The Nature of Managerial Work*. 1st edn. New York: Harper & Row, Publishers.

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

Naylor, J.C. and Dickinson, T.L. (1969) Task structure, work structure, and team performance. *Journal of Applied Psychology* 53(3): 167–177.

Power, M. (2007) *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

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

Robson, A. and Robinson, L. (2013) Building on models of information behaviour: Linking information seeking and communication. *Journal of Documentation* 69(2): 169–193.
Sarre, R. and Prenzler, T. (2005) Mapping the Australian security industry. *Security Journal* 18(4): 51–64.
Sennewald, C.A. (2011) *Effective Security Management*. 5th edn. Portland, OR: Butterworth-Heinemann.
Sjoberg, L. (2000) Factors in risk perception. *Risk Analysis* 20(1): 1–12.
Smith, C.L. and Brooks, D.J. (2013) Security Science: The Theory and Practice of Security. Waltham, MA: Elsevier.
Talbot, J. and Jakeman, M. (2009) *Security Risk Management Body of Knowledge*. Hoboken, New Jersey: Wiley.
Tushman, M.L. and Nadler, D.A. (1978) Information processing as an integrating concept in organizational design. *The Academy of Management Review* 3(3): 613–624.
Willis, H.H. (2007) Guiding resource allocations based on terrorism risk. *Risk Analysis* 27(3): 597–606.
Wood, R.E. (1986) Task complexity: Definition of the construct. *Organizational Behavior and Human Decision Processes* 37(1): 60–82.