1-1-2012

Corporate Security: Using knowledge construction to define a practising body of knowledge

David Brooks

10.1007/s11417-012-9135-1

This is an Author's Accepted Manuscript of: Brooks, D. J. (2012). Corporate Security: Using knowledge construction to define a practising body of knowledge. Asian Journal of Criminology, 8(2), 1-13. *The final publication is available at link.springer.com* here

Corporate Security: Using knowledge construction to define a practising body of knowledge

INTRODUCTION

The security industry is one of Australia's fastest growing sectors, generating revenues of approximately $4.5 billion per year and employing over 150,000 security personnel (Australian Security Industry Association, 2008). For example, census figures for a ten-year period from 1996 to 2006 demonstrated that while the Australian population increased by 12 percent and the police workforce by 15 percent, the number of security providers grew by 41 percent (Prenzler, Earle, Sarre, 2009, p. 3). However, *security providers* included many security occupations that would suggest that the comparison lacked some validity, an issue raised by Prenzler (2009, p. 4) that resulted in a more conservative figure of 26 percent. Nevertheless, even taking the more conservative figure, the security industry still out grew both the general population and more traditional security domains, namely public policing. In general, many parts of the world have seen a growth in private security (Prenzler, Martin, & Sarre, 2010).

The security industry in many parts of the world generates a significant value, for example in the United States the security industry is a business worth some $100 billion a year and still growing (ASIS International, 2005). Nevertheless, in contrast to other disciplines such as medicine and engineering, corporate security still lacks a concise definition and agreement on knowledge categories representing what constitutes its body of knowledge. Although corporate security has a clear function in protecting personnel, information and assets from harm, it is suggested by Fischer and Green (2004, p. 37) that corporate security has no universally agreed and cogent argument for definition. Furthermore, observation of corporate security education revealed that not much has been done to sum what constitutes the knowledge of corporate security (Nalla, 2001), an important issue when considering the increase in tertiary education based security programs. As a result, second career law enforcement and military personnel—who may lack the business background—were historically given priority when appointing corporate security managers, which led to marginalising and alienating the security function (Gill, 2007). In other words, security managers may lack business accruement and appropriate language for example risk management, cost-benefit analysis, etc., rather focusing on reactive security management such as physical security and investigations.

Purpose

The purpose of this study was to define one part of the larger security group, namely *corporate security*. This security group encompasses a significant proportion of those who provide protective security services throughout our society. Definition was achieved by the development and presentation of a docile body of knowledge based on past research and within an applied security domain.

Significance of the Study

One of the most important things learned in the last 20 years of study into the practice of security is how little is actually known, namely that the discipline of security has not yet matured (Giever, 2007). Nevertheless, there is an ever increasing reliance by both private and public sectors on private security, insomuch as in parts of the world such as Australia, Europe, New Zealand and North America, public police no longer have a monopoly on policing services (Bradley & Sedgwick, 2009, p. 468) and private security services have eclipsed police in number (Prenzler, et

al., 2010, p. 1). The challenge for the future is for security research to find a way of improving security practice (Gill, 2007). To invoke true professional status in the security industry, scientific decision-making must be practiced by the majority of practitioners (Calder, 2007, p. 3).

To gain such harmony among corporate security, practitioners' require a robust and consensual body of knowledge. However, there is a lack of tertiary level security education with most security management relevant courses offered at the vocational or technical college level (Prenzler et al., 2010, p. 1), which results in a lack of directed security research. In addition, there has been limited research in presenting a corporate security body of knowledge, with publications primarily by ASIS International (2003; 2009) and others (Brooks, 2009b; Hesse & Smith, 2001; Talbot & Jakeman, 2008). These limited publications are perhaps due to the diverse nature of security that makes research activity diffuse and security research difficult (Sarre, 2005), although there is supporting literature to develop such a body in many of the security domains.

The lack of a consensual corporate security definition has mandated research to sum the knowledge categories that represent the corporate security expert knowledge. Security professional expertise has never been more needed, as a true profession and consolidation of the term *corporate security* is crucial to the international community (Wakefield, 2007). This issue is becoming more significant as the many practising domains of security—such as public security, private security, national security, defence and private military security—converge in the current social and political environment. As Zedner states "scholars have tended to think about security within their immediate discipline and in detachment from one another" (2009, p. 3), highlighting the significance for this type of study.

Security is capricious in nature and practice, with multidimensional knowledge categorisation and heterogeneous occupations (Brooks, 2009a). Such diversity results in difficulty in providing a single encompassing definition for the many applied domains of security. Security cannot be considered singular in concept definition, as definition is dependent on applied context (Brooks, 2009b). One such applied security context is the domain of *corporate security*. Corporate security may be considered the practicing domain that provides security services and functions within either a public or private enterprise in the protection of the enterprise's valued assets. Nevertheless, this does not provide a clear definition of corporate security in the ability to be able to represent a concise and relevant body of knowledge.

The study provided a better understanding of corporate security, its body of knowledge and how its practicing knowledge categories may relate to each other. Such outcomes aid educational organisations to develop more concise and industry focused security pedagogy and curriculum, in particular at the tertiary level (Prenzler, et al., 2010). In addition the method of study resulted in spatial cluster formation that could result in presenting discrete educational paths, for example two or three fields of study within the corporate security domain. Corporate security is a multi-disciplined field and the identification of discrete education paths could help security specialisation. In turn, this would aid the development of practising corporate security professionals, equipped with proper knowledge and skills necessary to face current and future challenges in corporate security.

STUDY METHOD

The study was divided into two discrete phases (Figure 1). The first phase critiqued existing body of knowledge studies to develop an integrated framework of corporate security. The second phase tested this integrated framework using psychometric multidimensional scaling (MDS) knowledge mapping and from this analysis, produced a final framework.

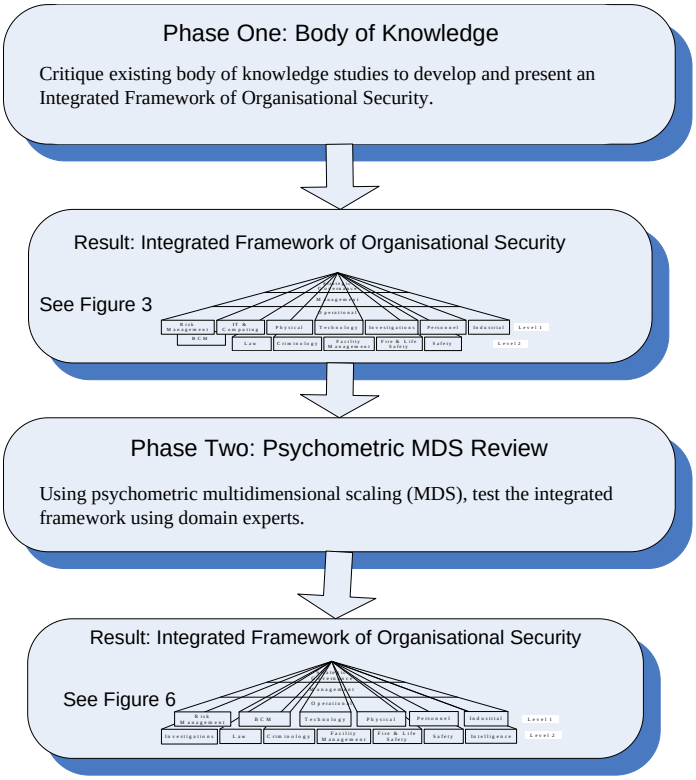

Figure 1: Study design

Phase two of the study, being the psychometric multidimensional scaling (MDS) knowledge mapping, used a web based survey instrument embedded with implicit security knowledge categories. Non-probabilistic selected Australian expert participants (n=27) made up the study's sampling group, with experts selected by their peers. In general, the participants consisted of people operating in private or public organisations at a managerial or executive level within their corporation's security group. In addition, a number of academics who are actively researching the security industry participated. Participants selected, on a sliding scale, how similar or dissimilar they considered pairs of knowledge categories (see Figure 2 for a sample).

		when compared to	Similar	1	2	3	4	5	6	7	8	9	10	Dissimilar
Security		Security management												
Security		Physical security												
Security		Security technology												
Security		ICT												
Security		IT security												
Security		BCM												

Figure 2: Sample of the MDS survey instrument.

MDS is a method that represents the pattern of proximities among pairs of objects (Borg & Groenen, 2005, p. 3). MDS is a statistical technique within the area of multivariate data analysis, "attracting worldwide interest" (Cohen, Manion, & Morrison, 2002, p. 369) and has been used in many other similar studies (Cox & Cox, 2000). The psychometric MDS knowledge structure technique, as demonstrated by Brooks (2009), provides a visual representation of similarities among measured knowledge categories. MDS analysis results in a spatial representation of knowledge concept clusters (Trochim, Cook, & Setze, 1994) and allows an analysis of judgements between variables to define dimensionality (Cohen et al., 2002). Within this study, these objects or variables were the security knowledge categories (Table 3). In support of MDS knowledge mapping, there has been many past studies that have considered knowledge structure from MDS analysis (Cheng, 2004; Martinez-Torres, Garcia, Marin, & Vazquez, 2005; Trochim, 2005b; Turner, 2002).

Data were extracted from the completed surveys, summed and inserted into Excel, considered the *source document*. At this point, validity and reliability measures were applied on the source data and a half-matrix formed. The half-matrix was inserted into Statistical Package for the Social Sciences (SPSS) for multidimensional scaling analysis, resulting in the spatial knowledge structure and further measures of reliability.

PHASE ONE: SECURITY BODY OF KNOWLEDGE

The study critiqued existing body of knowledge studies that focused on what could be considered corporate security. These studies included a criminal justice directed security course (Kooi & Hinduja, 2008), Integrated Framework of Organisational Security (Brooks, 2009b), Security Risk Management Body of Knowledge (Talbot & Jakeman, 2008) and the ASIS International Symposium (2009).

Kooi and Hinduja (2008) summarise their experience of teaching security to criminal justice undergraduates. The article considered the wider understanding of the *art and science* of security, resulting in the recommendation of nineteen topics areas (Table 1). Nevertheless, it could be argued that many of these proposed topics, for example retail, casino, Olympic, nuclear and museum security, may be considered practising areas of security, not security knowledge categories. Brooks (2008) describes such topic areas, proposing that practising areas should be classified within a knowledge category of *industrial security*. Industrial security could encompass industry specific aspects or functions related to security, for example within aviation security and the International Civil Aviation Organisation (ICAO) legislation. Corporate security education, from the perspective of criminal justice and social science academics, can be beneficial in further validating security categories and body of knowledge; however, such studies may also increase confusion as to what may constitute corporate security and reduce the ability of achieving consensus in the near to medium term.

Table 1: *Experimental security course: components in the context of a criminal justice undergraduate degree*

Security course components		
The origins and development of security	Security education, training, certification, and regulation	The role of security
Proprietary vs. Contract security	Risk analysis and security survey	Perimeter and exterior security
Interior Security and Access Control	Transportation/Cargo Security	Computer and Information Security
Security and the Law	Internal and External Fraud	Personnel Policies and

		Human Relations
Workplace Violence	Retail Security	Casino Security
Olympic Security	Nuclear Security	Museum Security
Continuity of Operations		

(Kooi & Hinduja, 2008, p. 299)

Brooks (2008; 2009b) investigated and critiqued 104 security related undergraduate security courses from Australia, South Africa, United Kingdom and United States. From this critique, seven courses were selected for in-depth course content analysis using Linguistic Inquiry and Word Count (Pennebaker, Francis, & Booth, 2001). This analysis resulted in 2001 security concepts being extracted, with the 14 more implicit concepts considered knowledge categories (Table 2). In addition, this study used other related body of knowledge studies (ASIS International, 2009; Bazzina, 2006) to support and valid these security related knowledge categories.

Table 2: *Corporate security knowledge categories*

Security categories description		
Criminology	Business continuity management	Fire science
Facility management	Industrial security	Information &computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

(Brooks, 2008, p. 19)

From these past studies and the 14 knowledge categories (Table 2), a proposed *integrated framework of organisational security* (Figure 3) was developed. The framework considered the breadth of corporate security, opposing many past studies that have presented a narrow approach to the diverse role of corporate security, such as Kooi and Hinduja (2008). Such breadth was supported by Yates (2007) when he stated that traditional security categorisation does not consider the large range of security related functions, including business continuity, emergency response, information security and risk management. As the integrated framework indicates, core or Level 1 security knowledge categories comprises of risk management, IT and computing, physical security, security technology, investigations, industrial security and security principles. Business continuity management may be considered a subordinate concept or risk mitigation strategy of risk management. The second level, or Level 2, may be considered allied or supporting disciplines or practising domains.

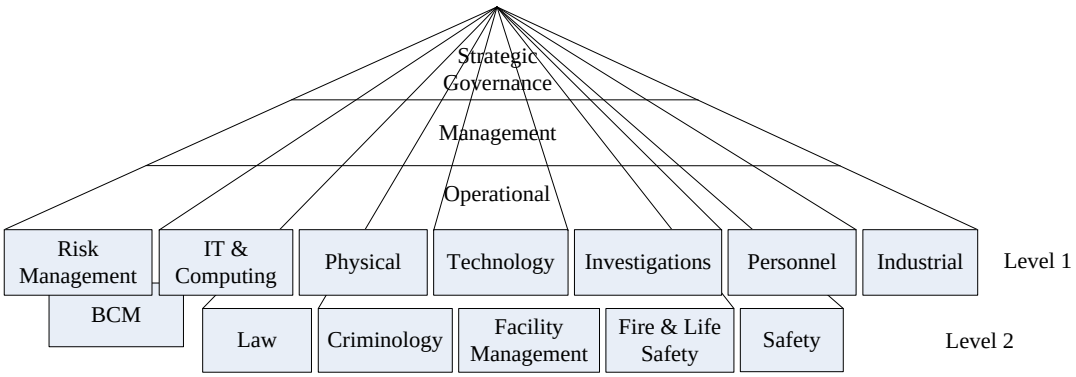

Figure 3: Integrated framework of corporate security. (Brooks, 2009b)

Note: BCM = Business Continuity Management, comprising of crisis, emergency and business recovery

The integrated framework may overlap other disciplines and practising domains, which is appropriate as other disciplines can and should inform and support corporate security. Supporting security knowledge categories may include law, criminology, facility management and safety, all disciplines with their own bodies of knowledge. In addition, the knowledge categories will overlap and support each other to a lesser or greater degree. As Young (2007) suggests, the more mature professional industry approach accepts levels of overlap that focuses on selectively drawing from related disciplines to append their unique offerings.

The ASIS International (2009) academic/practitioner symposium continues to develop a security body of knowledge. For example, the 2009 symposium attempted to gain an understanding of the security body of knowledge, understand what disciplines security may extract its knowledge categories from, what knowledge categories are core, how these knowledge categories can be used and to consider whether consistency and consensus can be gained? In addition, a list of 18 knowledge categories was put forward as the symposium's security model (Table 3).

Table 3: ASIS International Symposium security model

Security model		
Physical security	Personnel security	Information security systems
Investigations	Loss prevention	Risk management
Legal aspects	Emergency/continuity planning	Fire protection
Crisis management	Disaster management	Counterterrorism
Competitive intelligence	Executive protection	Violence in the workplace
Crime prevention	CPTED	Security architecture & engineering

(ASIS International, 2009)

PHASE TWO: EXPERT KNOWLEDGE STRUCTURE

Phase two tested the security knowledge categories and integrated framework in an attempt to measure how relevant these were according to experts; however, prior to phase two being

completed an initial proposition was put forward. The proposition suggested interrelationship of the knowledge categories, allowing interpretation to improve the consensus of the integrated framework.

The proposition put forward three significant outcomes. First, that the study could validate the 14 corporate security knowledge categories (Table 2) representing the security expert knowledge structure tabulated by Brooks (2008), subtracting or adding to these knowledge categories. Secondly, the study would present a psychometric multidimensional scaling (MDS) similarity map of the participating experts' corporate security knowledge structure. Thirdly, the spatial MDS similarity map could lead to cluster formation that indicated corporate security expert knowledge groupings and therefore, knowledge interrelationships of the measured knowledge categories (Alruwaii & Brooks, 2008).

In the study's proposition (Figure 4), it was suggested that *security* and *security management* would cluster and be the focal point of the spatial map. In addition and based on such expected close spatial similarity, *security* and *security management* would perhaps be found to be an interchangeable category. The knowledge categories of *investigations* and *fire science* may respectively be closely related to *criminology* and *facility management*, representing two separate category clusters. Furthermore, that *business continuity management* (BCM) would be subordinate to *risk management* (as shown in Figure 3) and therefore, these concepts would be clustered together. For illustration purposes, Figure 4 provides a speculative view of the propositional corporate security knowledge categories spatial structure.

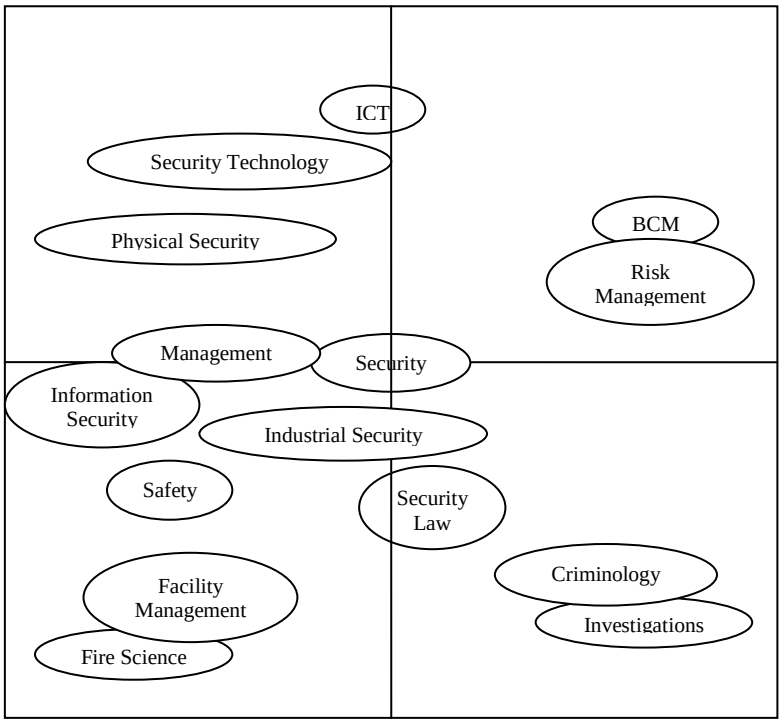

Figure 4: Speculated spatial structure of corporate security knowledge categories. (Alruwaii & Brooks, 2008)

Other knowledge category relationships could be the cluster of technologies, such as *security technology*, *physical security* and *information communications technology* (ICT). Talbot and Jakeman (2008) states that the knowledge category *information and computer* should be divided into two discrete categories, namely *information security* and *information communications technology*. By separating these two categories, it was expected that information security would cluster with security management, as information security may be considered more procedural in function than technical. The MDS psychometric map could test, according to the participating experts, the significance of such views.

MDS analysis of the expert knowledge structure

The study analysis and following interpretation of the source data resulted in a spatial multidimensional scaling (MDS) map of the participating experts' knowledge structure (Figure 5). There were some interesting aspects to the spatial locality of some of the corporate security knowledge categories, such as *investigations*, the cluster of technology categories, the relationship of *risk management* and *business continuity management*, and locality of *industrial security*. What was expected was the central locality of *security*, being the most abstract and ordinate knowledge category.

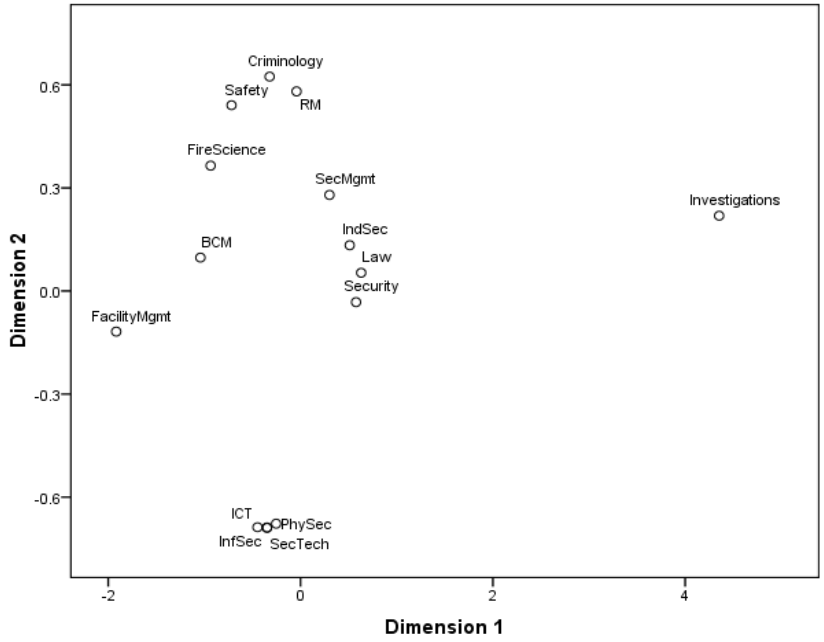

Figure 5: MDS expert knowledge structure of corporate security.

When considering Figure 5, the categories of *security* and *security management* were both located relatively centrally in respect to the other knowledge categories, indicating more abstract and central ideas; however, these categories were not clustered as the study's proposition suggested (Figure 4). In addition, the categories of *law* and *industrial security* were located between these two categories. Why *law* was located in such a locality would require greater research, perhaps with

greater in-depth interviews with the expert participants. However, it is postulated that law may be spatially located at this point because it is a fundamental principle by which society and its members exists, and is therefore a foundation for security. Nevertheless, the locality of industrial security appeared to indicate that this category was not clearly understood in respect to definition, supported by such comments from the participating experts.

The technology categories of *physical security*, *security technology*, *ICT* and *information security* were spatially clustered, indicating similarity of concepts and that these functions are closely related. Nevertheless, it was proposed that *information security* was not necessarily a technology category, related more to *security management* as a procedural function. As Talbot and Jakeman (2008) states, the knowledge category *information and computer* should be divided into two discrete categories, namely *information security* and *information communications technology* (ICT); however, according to the MDS knowledge structure these were viewed as similar categories and should perhaps remain as one knowledge category.

Investigations was found to be an outlier, relatively separated from the other knowledge categories. Based on this locality, it could be suggested that investigations is not a significant knowledge category of corporate security. Finally, in the proposition it was put forward that *risk management* and *business continuity management* (BCM) would be similar and would therefore cluster together. The MDS knowledge structure placed these two categories relatively apart from each other, indicating that the experts viewed these categories as quite discrete functions (Table 4).

Table 4: *Interpretations of MDS knowledge structure*

Knowledge category	MDS interpretation
Security	Central location due to its ordinate position
Security & security management	Only some degree of cluster, indicating discrete categories
Industrial security	Located between security and security management, indicating no clear category definition
Investigations	Spatial outlier, indicating that this is not a core category
Physical, ICT, information security & security technology	All concepts clustered, indicating a common knowledge category
Information security	Clustered with technology, indicating that this should be integrated with Computing & Information Technology
Risk Management & BCM	Spatial separation, indicating distinct functions

The reliability and validity of the MDS knowledge structure was demonstrated through a number of measures. First was the central spatial locality of *security*, having been put forward in the study's proposition as accommodating this locality being the most abstract and ordinate category. The MDS goodness of fit (SSTRESS1) indicated an acceptable result (SSTRESS1=0.222) for this type of date analysis. In addition, the reliability measure on the *source data* demonstrated a high reliability measure of 0.992 (Cronbach Alpha).

INTEGRATED FRAMEWORK OF CORPORATE SECURITY

Reflecting from the results and interpretations of the MDS expert knowledge structure of corporate security (Figure 5), the integrated framework of corporate security (Figure 3) was adjusted. Adjustments to the framework included the relocation of *business continuity management* to Level 1 and *investigations* to Level 2. The categories of *security technology* and *information technology and computing* were integrated into a single category of *security technology*, comprising such

technologies as IT networks, firewalls, CCTV, access control, intrusion detection systems, etc. From discussions with the participating experts, it was suggested that *security intelligence* should be included as a supporting corporate security category. Adjustments to the integrated framework resulted in the final integrated framework of corporate security (Figure 6), considered as *Security Science*.

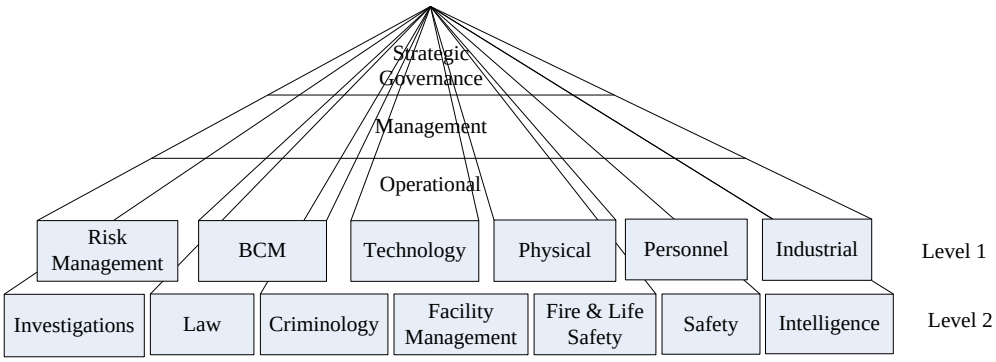

Figure 6: Integrated framework of corporate security or Security Science.

Notes: BCM = Business Continuity Management; Technology = security technology, information technology and computing

The ASIS International body of knowledge (ASIS International, 2009) security model (Table 3) further supported the inclusion of many of the study's defined categories and to some degree, the integrated framework of corporate security (Figure 6). For example, Business Continuity Management (BCM) encompasses the security model's categories of emergency/continuity planning, crisis management and disaster management categories. Therefore, from the 18 proposed categories from the ASIS International security model, five categories are presented in Level 1 and three are in Level 2. Nevertheless, it is argued that the ASIS International security model categories such as crime prevention through environmental design (CPTED), crime prevention and counter-terrorism are tasks or functions embedded within the prescribed knowledge categories.

The expected outcomes of the study put forward in the proposition were achieved; namely that the 14 corporate security knowledge categories (Table 2) were further validated and resulting in the adjustment of some knowledge categories. The study presented the psychometric multidimensional scaling (MDS) map (Figure 5) of the participating experts' corporate security knowledge structure, allowing adjustment and further validation of the integrated framework of corporate security or Security Science (Figure 6).

RECOMMENDATIONS

The study outcomes led to a series of recommendations in how the proposed framework informs understanding of the corporate security domain and directs further inquiry. These recommendations suggest how the framework may benefit both academia and professional understanding of this security domain including defining domain boundaries, gaining a greater understanding of expert knowledge structure, assisting in developing a singular security body of knowledge, improving security directed pedagogy and curriculum, and providing directed development of the domain of corporate security. Finally, the framework may assist in supporting the view that the domain of corporate security could develop its own scholarly domain of inquiry considered Security Science.

Security lacks definition (Tate, 1997), is defuse and yet is a distinct field of practice and study (ASIS International, 2003; Brooks, 2009b) supported by professional security bodies such as the ASIS International, Risk Management Institute of Australasia (RMIA) and many other industry groups. Nevertheless, the security industry is a diverse and speciality industry that has a requirement for both generic and domain specific skills (Hesse & Smith, 2001; Manunta, 1996) and being a relatively young and emerging discipline, continues to expand (Fischer & Green, 2004; Tate, 1997). Therefore, corporate security has to have a clear understanding of its operating boundaries, from which further consensus in a body of knowledge will be achieved. There are many overlapping and defuse security domains that interact, interrelate and have independencies with corporate security, such as policing, national security, military security and private security, to name just a few.

There is still further work required in gaining consensus in knowledge category definition and a corporate security body of knowledge; however, it could be suggested that both are required to achieve the other. For example, this study found an issue with the experts' understanding of the category *industrial security*. Nevertheless, continued body of knowledge research from such groups as ASIS International, and the development of national and international professional groups will ultimately result in such common understanding.

At the tertiary level, many corporate security courses have been developed from related disciplines, being police, justice or criminology studies (Smith, 2001b; Tate, 1997). In addition, many relevant courses in corporate security are only offered at the vocational level, restricting the industry professionalism and informed research. This opposes views from industry groups such as ASIS International, who suggest that many allied disciplines should be separate and discrete from security (2003, p. 4). At the tertiary level there is a lack of academic security programs, with most focused on criminal justice, crime prevention, risk management (Jay, 2005; Manunta, 1996; Prenzler, Martin, & Sarre, 2010), security studies or politcial science. Such distortion of the corporate security discipline will result in security research that is not necessarily appropriate for the security industry, reducing the ability of the industry to use evidence based mitigation strategies.

Nevertheless according to Smith, security knowledge is being established though the development of appropriate domain concepts (2001a, p. 32), a view supported by Simonsen who stated that the "body of knowledge of security has grown rapidly in the past decade" (1996, p. 230). By developing such defined knowledge and supporting this with vigorous research inquiry, it could be argued that the domain could develop its own distinct scholarly area of study. Research studies are required to feed into tertiary educational institutes, inform pedagogy and develop curriculum. If this is achieved, increasing tertiary educational institutes will offer relevant courses, applied practising boundaries will be better understood and the industry will drive toward understanding and later, professionalism.

CONCLUSION

Security is diverse in nature and practice, with heterogeneous occupations. Such diffusion results in the need to define various operational parts of security, achieved to some degree through a body of knowledge. The study put forward an integrated body of knowledge framework of Corporate Security (Figure 6), developed from core security knowledge categories and with integration from other body of knowledge studies. The study used multidimensional scaling (MDS) to present a spatial knowledge structure of the participating security experts. Such a knowledge structure allowed the implicit expert understanding of the security categories to be analysed, displayed and interpretations made, resulting in a number of category interrelationships. It was found that *security* was the most ordinate concept; however, *security management* was discrete from *security*. There were a number of closely related categories, namely *physical security*, *information security*, *security*

technology and *information communications security*, considered as *security technology*. The category of *investigations* was found to be an outlier, indicating that this category was not a core function for corporate security.

The MDS knowledge structure also allowed the integrated framework of Corporate Security to be adjusted to better reflect experts' views. This approach resulted in a two-level structure to the framework, with core corporate security categories as Level 1 and allied or supporting categories as Level 2. Nevertheless, it should be noted that there will be a degree of overlap between each knowledge category and level, as these categories are not hierarchical or applied in isolation. The study considered the need to present a practical and industry focused Corporate Security consensual body of knowledge, considered *Security Science*. It is suggested that the study outcomes could improve Corporate Security comprehension, define its operating boundaries, aid educational institutions to better offer and deliver corporate security curriculum, and support the advancement of the security profession.

REFERENCE LIST

Alruwaii, A., & Brooks, D. J. (2008). Organisational security: a propositional study to map expert knowledge. *Proceeding of the 1st Australian Security and Intelligence Conference* pp. 4-11). Perth.

American Society for Industrial Security. (2002). *Proceedings of the 2002 academic/practitioner symposium*. The University of Cincinnati, Ohio: ASIS International.

Angus & Roberston. (1992). *Dictionary and thesaurus*. Sydney: Harper Collins Publishers.

ASIS International. (2003). *Proceedings of the 2003 academic/practitioner symposium*. The University of Maryland, Maryland: ASIS International.

ASIS International. (2005). *Career opportunities in security*. Alexandria, VA: ASIS International.

ASIS International. (2009). Security body of knowledge (BoK): Substantive considerations. Unpublished ASIS International Academic/Practitioner Symposium 2009, ASIS International.

Australian Security Industry Association. (2008). Security industry overview. Retrieved 2 September, 2008, from http://www.asial.com.au/default.asp?page=%2Fconsumer+information%2Fsecurity+industry+overview

Bazzina, M. (2006). *Security standards and support systems report: A collaborative project between the Commonwealth Attorney-General's Department and Standards Australia*. Sydney: Standards Australia International Ltd.

Borg, I., & Groenen, P. J. (2005). *Modern multidimensional scaling: theory and applications* (2nd ed.): Springer.

Bradley, T., & Sedgwick, C. (2009). Policing beyond the police: A "first cut" study of private security in New Zealand. *Policing and Society, 19*(4), 468-492.

Brooks, D. J. (2008). Defining the science of security through knowledge categorisation. *Acta Criminologica, CRIMSA Conference Special Edition 2008, 1*, 12-23.

Brooks, D. J. (2009a). *Key concepts in security risk management: A psychometric concept map approach to understanding*. Saarbrucken: VDM Verlag.

Brooks, D. J. (2009b). What is security: Definition through knowledge categorisation. *Security Journal, DOI 101057/sj.2008.18*, 1-15.

Calder, J. D. (2007). Been there but going where? assessing old and new agendas in security research and study. *Security Journal, 20*, 3-8.

Cheng, C. C. (2004). Statistical approaches on discriminating spatial variation of species diversity. *Botanical Bulletin of Academia Sinica, 45*, 339-346.

Clancey, W. J. (1997). The conceptual nature of knowledge, situations, and activity. In P. J. Feltovich, K. M. Ford & R. R. Hoffman (Eds.), *Expertise in context: Human and machine* (pp. 247-291). Menlo Park, CA: The MIT Press.

Cohen, L., Manion, L., & Morrison, K. (2002). *Research methods in education* (5th ed.). London: RoutledgeFalmer.

Cox, T. F., & Cox, M. A. A. (2000). *Multidimensional scaling: Monographs on statistics and applied probability* (2nd ed. ed. Vol. 88). Boca Raton: Chapman & Hall/CRC.

Eysenck, M. W., & Keane, M. T. (2002). *Cognitive psychology: A student's handbook* (4th ed.). New York: Psychology Press Ltd.

Ferguson, G. (2004, August). Homeland security: Emerging technologies: Policing conference returns to Adelaide. *Australian Defence Magazine, 12*, p. 54.

Fischer, R. J., & Green, G. (2004). *Introduction to security* (7th ed.). Boston: Butterworth Heinemann.

Giever, D. (2007). Security education - past, present and the future. *Security Journal, 20*, 23-25.

Gill, M. (2007). The challenges for the security sector: thinking about security research. *Security Journal, 20*, 27-29.

Hesse, L., & Smith, C. L. (2001). Core curriculum in security science. *Proceedings of the 5th Australian Security Research Symposium* pp. 87-104). Perth, Western Australia.

Jay, C. (2005, 2005, 17 March). Big debacles help shape a new science. *The Australian Financial Review*, p. p. 2,

Kellogg, R. T. (2003). *Cognitive psychology* (2nd ed.). Thousand Oaks: Sage Publications.

Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. *Journal of Criminal Justice Education, 19*(2), 290-307.

Kruskal, J. B., & Wish, M. (1978). *Multidimensional scaling* (Vol. 07). London: Sage Publications.

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

Martinez-Torres, M. R., Garcia, F. J. B., Marin, S. L. T., & Vazquez, S. G. (2005). A digital signal processing teaching methodology using concept-mapping techniques. *IEEE Transactions on Education, 48*(3), 422-429.

Morley, H. N., & Vogel, R. E. (1993). The higher education dilemma for the private security professional: Delivery methodologies and core curriculum from the practitioner's perspective. *Security Journal, 4*(3), 122-127.

Nalla, M. K. (2001). Designing an introductory survey course in private security. *Journal of Criminal Justice Education, 12*(1), 35-52.

Novak, J.D., & Gowin, D. B. (1984). *Learning how to learn.* Cambridge: Cambridge University Press.

Pennebaker, J. W., Francis, M. E., & Booth, R. J. (2001). *Linguistic inquiry and word count (LIWC2001)*. Mahwah, NJ: Erlbaum Publishers.

Prenzler, T., Earle, K., Sarre, R. (2009). Private security in Australia: Trends and key characteristics. Trends and Issues in Crime and Criminal Justice, no. 374 [Electronic Version]. Retrieved 11 August 2010, from http://www.aic.gov.au/publications/tandi/tandi374.html

Prenzler, T., Martin, K., & Sarre, R. (2010). Tertiary education in security and policing in Australia. *Asian Journal of Criminology, 5*, 1-10. doi: 10.1007/s11417-009-9074-7

Sarre, R. (2005). Researching private policing: Challenges and agendas for researchers. *Security Journal, 18*(3), 57-70.

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

Smith, C. L. (2001a). Security science as an applied science? *Australian Science Teachers' Journal, 47*(2), 32-36.

Smith, C. L. (2001b). Security science: An emerging applied science. *Journal of the Science Teachers Association of Western Australia, 37*(2), 8-10.

Talbot, J., & Jakeman, M. (2008). *SRMBOK: security risk management body of knowledge*. Carlton South: Risk Management Institution of Australasia Ltd.

Tate, P. W. (1997). *Report on the security industry training: Case study of an emerging industry*. Perth: Western Australian Department of Training. Western Australian Government Publishing.

The Interim Security Professionals Taskforce. (2008). *Advancing security professionals: a discussion paper to identify the key actions required to advance security*. Melbourne: The Australian Government Attorney-General.

Trochim, W. M., Cook, J. A., & Setze, R. J. (1994). Using concept mapping to develop a conceptual framework of staff's views of a supported employment program for individuals with severe mental illness. *Journal of Consulting and Clinical Psychology, 62*(4), 766-775.

Trochim, W. M. K. (2005b). Concept mapping. Retrieved 28 July 2009, from http://www.socialresearchmethods.net/kb/conmap.htm

Turner, P. (2002). Multidimensional scaling analysis of techniques used by physiotherapists in Southeast Australia: A cross-national replication. *Australian Journal of Physiotherapy, 48*, 123-130.

Wakefield, A. (2007). The study and practice of security: today and tomorrow. *Security Journal, 20*, 13-14.

Yates, A. (2004). *Australia's homeland security market and industry's role*. Canberra: Australian Homeland Security Research Centre.

Yates, A. (2007). *The future of private security*. Canberra: Australian Homeland Security Research Centre.

Young, L. J. (2007). Criminal intelligence and research: An untapped nexus. *The Journal of the Australian Institute of Professional Intelligence Officers, 15*(1), 75-88.

Zedner, L. (2009). *Security: Keys ideas in criminology*. London: Routledge.