1-1-2011

Mapping the organizational relations within physical security's body of knowledge: a management heuristic of sound theory and best practice

Richard Coole
Edith Cowan University

David J. Brooks
Edith Cowan University

DOI: 10.4225/75/57a012aaac5c3
4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

MAPPING THE ORGANIZATIONAL RELATIONS WITHIN PHYSICAL SECURITY'S BODY OF KNOWLEDGE: A MANAGEMENT HEURISTIC OF SOUND THEORY AND BEST PRACTICE

Michael Coole and David J Brooks
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
m.coole@ecu.edu.au; d.brooks@ecu.edu.au

Abstract

Security Science education at university levels is still in its infancy, with little agreement towards knowledge, curriculum and competency. Therefore, it is essential that educators draw on relevant literature highlighting means of efficient and effective knowledge transfer for tertiary students within the Security Science domain. Such knowledge transfer will reduce the gap between academic knowledge (explicit) and professional competency (tacit knowledge). This paper presents phase one of a multiphase study.

A qualitative "systems based knowledge structure" of security domain categories has been conceptually mapped as a domain heuristic. The heuristic drew on research highlighting that experts have both richer depths of domain knowledge and superior cross referenced organizational structure. The conceptual map takes a top-down approach bounded by routine activity, rational choice, situational crime prevention, defence in depth, security decay and management theories within the elements of prevention, preparedness, response and recovery. Results indicate that within a systems approach, core security professional competencies relate to the ability to skilfully apply the theories and best practice principles represented within the preliminary heuristic that brings together academic theory with practising security strategies.

Keywords

Security Science; education; knowledge; learning; theories; best practice; heuristic

INTRODUCTION

Professional knowledge is based on combinations of explicit and implicit domain specific knowledge, used in such a way that an individual can solve new problems within a professional domain by drawing on existing cognitive structures. The developing profession of Security Science requires a means of transferring domain category knowledge in an efficient and meaningful manner for enhanced problem solving capabilities. It is therefore essential that novice learners (students) within the security domain are explicitly presented with an organizational structure of physical security knowledge categories to ensure they are able to employ a rich framework of cross referenced concepts in their future problem solving endeavours.

Educators in the physical security fraternity have always recognised the need for experience in robust learning. However, this paper argues that the gap between explicit and implicit learning can be reduced by drawing on the literature of expertise, specifically, security experts. Experts not only have a rich volume of domain knowledge, supported through many years of practical experience, but their knowledge is strongly cross referenced with a rich network of connections between domain concepts. Such highly organized domain concepts facilitate more efficient retrieval for professional problem solving. This paper presents such an organized knowledge structure through the use of a physical security domain concept map. Such a map is focused towards developing more meaningful learning at the conceptual level, therefore enhancing the journey from novice to competent security professional.

Objective

The objective of this paper is to respond to the question: *What are the core professional competencies for a security professional and where are they drawn from*? The work considers the premises of Manunta (1999), Burke (cited in Griffiths, Brooks & Corkill, 2011, p. 2), the Australian Interim Security Professional's Task Force (2008) and the earlier works of William's (1981), who proposed a "security systems design philosophy" to

present an explicit knowledge based, functional top-down system philosophy (heuristic) as an educational tool (schemata) for Security Science novice learners.

IS SECURITY DEVELOPING AS A PROFESSION?

Industry professionals have become essential to the very functioning of modern society. As Donald (1983, pp. 3-4) highlighted "we look to professionals for the definition and solution of society's problems". Within the security domain the Australian Interim Security Professional's Task Force (2008) identified security professionals as senior people working in the operational and strategic sector of the security industry. The task force further defined security professionals as a group critical in supporting the protection of government, commercial organisations, non-government organisations and the community. However, the task force highlighted that security professionals have not been able to contribute their full potential to the nation's security and safety, primarily due to a lack of clear understanding of either the profession or security professionals. In addition, Donald (1983, pp. 4-5) points out that as a society we see and experience failures of professional action, resulting in the loss of public confidence and calls for external regulation of professional activity. Recently, attention has been focused towards identifying the core professional competencies of security professionals. However, as Brooks (2010, p. 225) points out, security is a diverse and multi-disciplinary profession with a wide spectrum of activities and skills.

Security's diversity has resulted in a lack of professional consensus relating to a definition (Borodzicz & Gibson, 2006, p.182; Manunta, 1999, p. 58) and arguably, professional standing. As Borodzicz and Gibson (2006) suggest, the concept of security can have different meanings depending on context. For example, Manunta (1999, p. 58) argues that the variety of security's descriptive definitions are inadequate, purporting that security must be considered by a more functional, clearer definition. Such a view is supported by Burke (cited in Griffiths, Brooks & Corkill, 2011, p. 2) who argues that for security to be useful it must be defined in terms of its practices.

In considering diversity in both approach and definition, Brooks (2008, p. 5) argued that security may only achieve definition through applied context and concept definition, where definition may be achievable through a consensual body of knowledge. In considering definitional barriers and discordant views, two common professional threads are supported. Firstly, there is a desire on the part of practitioners to protect assets that they hold to be valuable from deliberate malicious human intervention through a variety of countermeasures (Borodzicz & Gibson, 2006, pp. 181-182). Second and from a functional perspective, for security to be effective it must be implemented within a "*systems*" approach (Underwood, 1984; Fennelly, 1997; Fisher & Green, 2003; Garcia, 2001).

Developing a Security Science body of knowledge

Wilensky (1964, p. 138) highlighted that for an occupation to assert professional authority it must first find a technical basis, assert an exclusive jurisdiction, link both skill and jurisdiction to standards of training, and convince the public that its services are uniquely trustworthy. To these points the Australian Interim Security Professional's Task Force (2008) accepted that for security to be considered a profession, it must include the characteristics of a distinct body of knowledge, agreed and enforced standards of behaviour/ethics, standards of education, formal requirement for professional development and a college of peers; yet to date this has not occurred. Wilensky (1964, p. 138) argued that the success of a claim for professional is greatest where the society evidences strong wide spread consensus regarding the knowledge or doctrine to be applied.

A study by Brooks's (2007) presented fourteen hierarchical security subject categories (Table 1) across many associated industries within many occupations. These subject categories hierarchically represent the salient practice areas in which security as a discipline draws its body of knowledge.

Table 1. Hierarchical security domain subject categories

Security domain subject category descriptors		
Criminology	BCM	Fire science
Facility management	Industrial security	Information & Computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

Brooks (2006, p. 173) highlights that whilst security practitioners originate from many disciplines, security experts hold a rich knowledge structure. Such a view is congruous with studies highlighting that a large or organized body of domain knowledge is a prerequisite to expertise (Bedard & Chi, 1992, p. 135). Conversely, within the context of tertiary education, Lussier (2006, p. 22) highlights that many graduates do not know how to employ academic knowledge.

Furthermore, Vu, Rigby, Wood and Daly (2011, p. 3) highlight that strong research-based evidence exists that professional employability requires graduates to be able to demonstrate their achievement of graduate attributes in order to enable novice learners to apply their knowledge critically and reflectively. As Nalla and Morash (2002, p. 9) point out, core ideas must be passed on to students within a discipline for them to succeed. This view leads to the question; what are the core professional competencies for security graduates and professionals and where do they come from? To the latter, Wilensky (1964, p. 144) suggested that as an occupation moves towards professional standing, its formal training schools at some stage either begin or seek out university involvement where there is a steady development of standards in study, academic degrees and research programs to expand the knowledge base. This development for security at the tertiary level is still in its infancy, with limited consensual agreement on content requirements (Brooks, 2010).

Accordant with such discourse, The Australian Interim Security Professional's Task Force (2008, p. 10) asserted that the Australian security profession has a distinct body of knowledge. However, a characteristic of professional knowledge is how knowledge is applied varies with the situation (Stake, 2010, p. 13). For example, Stake (2010, p. 13) explains professional work depends on science, but each profession has its own separate body of knowledge. It is therefore considered that professional knowledge differs from scientific knowledge, although overlaps exist. Cornford and Athanasou (1995, p. 12) suggest the situation can be summed on a continuum (Figure 1).

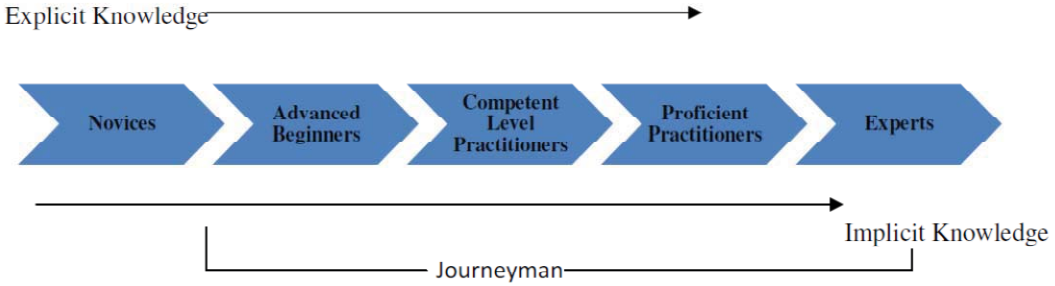

Figure 1. The professional development continuum

(Cornford & Athanasou, 1995, p. 12)

According to Wilensky (1964, pp. 149-150) the optimal base of knowledge or doctrine for a profession is a combination of intellectual and practical knowing, some of which is explicit (classifications and generalizations learned from books, lectures and demonstrations), and some implicit (understanding acquired from supervised practice and observation). Wilensky's (1964, pp. 149-150) views are supported by Griffiths, Brooks and Corkill (2011, p. 3) who highlight that professional bodies of knowledge are both academic and practical requiring both education and training to be passed on.

Within such a continuum, novices seek logical, fairly consistent all purpose rules to guide their behaviour (Cornford &, Athanasou, 1995, p. 12). Furthermore, novices start with little domain knowledge and use weak methods to solve problems (Eysenck & Keane, 2001, p. 421), whilst advanced beginners start to employ experience problem solving processes. Competent level practitioners exercise greater authority in problem solving, they set priorities and make plans, they determine what is important and understand that the order of priority may change. Nevertheless, proficient practitioners may no longer consciously think about adjustments, for them intuition or "know-how" becomes important.

It can be argued that for security advice to be professional—that is soundly based in theory and established practice (norms)—then identifying core security competencies means highlighting its explicit domain knowledge structure. Furthermore, these combined characteristics must be cross referenced with a rich network of connections amongst the subordinate concepts and represented collectively as an organised system from a top-down (theory/practice) approach. Security is more practitioner-oriented (Nalla & Morash, 2002, p. 9), therefore these core norms (knowledge structure) are focused towards various processes, measures, functions and tasks which are considered essential.

UNDERLYING THEORY

Epistemology is the theory of knowledge; the critical study of its validity, methods and scope (The Collins Concise Dictionary, p. 417). The central concern of epistemology is the growth of knowledge (Fraser, 1993, p. 16). Consistent with such literature, the underlying theory for this study is trivial constructivism within the assimilation theory paradigm. Constructivism holds that knowledge is constructed (not discovered) based on previous knowledge and is evolving over time (Novak, 1993, p. 167); where trivial constructivism recognises that new ideas are built on the foundation of prior ideas (Fraser, 1993, p. 16). That is, knowledge has structure, a history of creation and affective connotations (Novak, 1993, p. 171).

According to Novak (1993, pp. 171-172), Ausubel's (1963) assimilation theory placed central emphasis on cognitive processes involved in knowledge acquisition and the role that explicit concept and propositional frameworks play in knowledge acquisition. From the standpoint of formal education, Ausubel, Novak and Hanesian (1968, pp. 21-27) highlight clearly distinct forms of learning. That is, the distinction between reception and discovery learning and between rote and meaningful learning. Ausubel, et al, (1968) articulates the viewpoint that most of the understandings learners acquire both in and out of formal schoolings are presented rather than discovered. In reception learning (rote and meaningful) the entire content to be learned is presented in its final form. Thus, students are not required to engage in independent discovery; learners are only required to internalize and incorporate the material for availability and recall at some later time. For meaningful reception learning the potential meaningful task or material is comprehended by the student or made meaningful in the process of internalization.

In contrast, discovery learning incorporates an essential feature—the principle content is not presented—but must be discovered by the student before it can be meaningfully incorporated into the learner's cognitive structure. According to Ausubel, et al, (1968, p. 24) the first phase of learning by discovery requires a different process from that of reception learning. First, learners must rearrange information, integrate it with existing cognitive structures and reorganize or transform the integrated combination in such a way that they can generate a desired-end-product or discover a missing means-end relationship. After such learning is complete, the discovered content is made meaningful in much the same way as that presented content is made meaningful in reception learning.

Evaluating these different learning modes Ausubel, et al, (1968, p. 26) argues that discovery learning, or discovery methods of teaching are not an efficient primary means of transmitting the content of an academic discipline. Ausubel (1963) rejected the role of discovery learning arguing that reception learning could lead to more meaningful learning; putting forward the idea of an advanced organizer which could serve as a cognitive bridge between new knowledge to be learned and existing relevant concepts and propositions in the learner's cognitive structure (Novak, 1993, p. 172). According to Fraser (1993, p. 31) a constructivists approach within assimilation theory posits that learning is in essence a process of making connections, or seeing relationships.

METHODOLOGY

This paper presents phase one of a multi-phased study. Phase one applied a qualitative literature critique, which draw on the underlying theory of constructed knowledge to present a preliminary cross-referenced concept map (organized structure) of security professional's knowledge category connections. Working on the underpinnings of constructivism (Novak, 1993, p. 175), concept mapping has been supported as a useful tool (heuristic) in both planning instruction, helping students learn how to learn and to illustrate key ideas. That is, concept maps articulate the key concepts and propositions of a subject matter and their interrelationships. Concept (cognitive) maps are hierarchically ordered from a "top-down" approach.

The literature critique presented a design and planning heuristic as a rich network of cross referenced connections amongst security concepts (theory/ practices) as an organised body of knowledge for future security professionals. Such an approach is consistent with the Australian Interim Security Professional's Task Force (2008), using both established theory and best practice approaches stemming from within defined knowledge categories (Brooks, 2010).

RESULTS

A concept map was developed, commencing as an all encompassing "top down" model towards protective security (Figure 2). This model is consistent with the Australian Government's approach to security (2008, p. III), represented within the elements of *Prevention*, *Preparedness*, *Response* and *Recovery*. Such an approach is accordant with Underwood's (1984, pp. 3-4) two type offender typology, encompassing opportunistic and

deliberate offenders. Underwood's (1984) deliberate adversary model highlights the need to prevent purposeful actions against organisational, commercial or governmental objectives. From there, to be prepared in case such actions manifest, to respond and when negative affects manifest, recover in the shortest possible time to reengage business objectives (HB 167, 2006, pp. 63-64). Thus, such a model is located at the top of the hierarchical structure of the concept map.

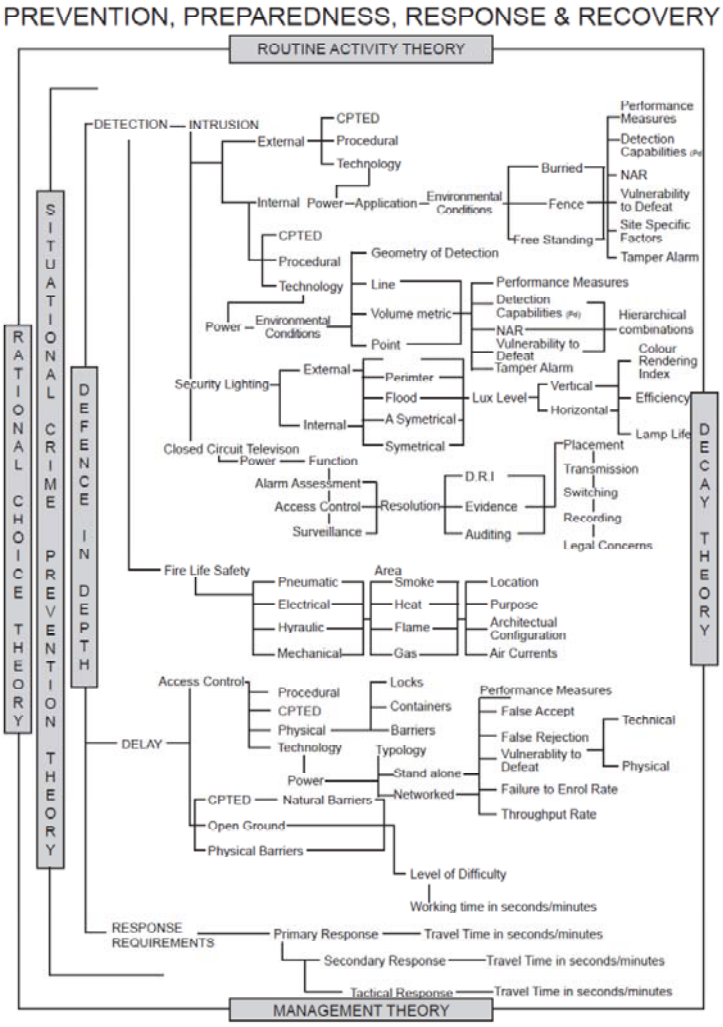

Figure 2. Preliminary conceptual map of security theory driven knowledge domains

Prevention and Preparedness

The first elements "prevention and preparedness", requires the concept to be able to "stop" an action outcome. This requirement draws on Routine Activity Theory (RAT) (capable guardian), where it is argued that suitable security controls alter the likelihood of convergence in space and time of motivated offenders, suitable target and an absence of capable guardian against attack (Cohen & Felson, 1979, p. 589). RAT is considered within the Rational Choice Theoretical (RCT) frame, which considers the cost benefits of an adversary action (expected utility). This approach entwines concepts such as taste (or distaste) and preference for the offence, moral values, proclivity for violence and preference for risk (Winoto, 2003, p. 2).

Rational cues not to offend against protected assets employ situational variables or Situational Crime Prevention theory (Clarke, 1980, pp. 138-140), where offenders respond to the chances of being detected (detection), the difficulty in achieving the task (delay) and the chances of being caught (response) achieved through defence in depth. Defence in depth is underpinned by the elements of detection, delay, response and recovery. In addition, within the detection element, security is interwoven with fire life safety within a public security approach (Cohn, 1981, p. 99; Craighead, 2003, pp. 22-24) and therefore, detecting fire must be considered. Consistent with the response element of prevention, preparedness, response and recovery, and defence in depth, there must be a means for executing various levels of response for adversary actions including primary, secondary and where necessary tactical response capabilities (Garcia, 2006, pp. 237-246).

Once individual elements of defence in depth have been commissioned within a systems approach (Kovacich & Halibozek, 2006, pp. 37-46), the measurable process that achieves security needs to be considered. This relates to the individual measures that achieve holistic security (Garcia, 2001; 2008), which need to be established and maintained at their commissioned levels of effectiveness. As such, the top down approach must also include decay theory (Coole, 2010, pp, 234-235). This aspect requires management theory, which considers that managers are responsible for achieving organisational objectives through the efficient utilization of resources, underpinned by functions such as planning, organising, leading, controlling (Lussier, 2006, pp. 6-19), compliance (Kovacich & Halibozek, 2006) and span of control (Sennewald, 2003, p. 59). Given that a physical protection system combines people, procedures and equipment management theory must be considered in achieving a successful output for the system.

Best Practice Approach to Security Systems

Consistent with Umibe (1991, p. 359) and the Australian Interim Security Professional's Task Force (2008), the preliminary conceptual map of theory driven security category knowledge domains is supported by best practice approaches towards achieving a top-down systems based approach to physical security (Figure 3). Best practice approach commences with a threat analysis ensuring the system is threat driven (Williams, 1981, p. 142; Sennewald, 2003, p. 196; HB 167, 2006, p. 40; Talbot & Jakeman, 2009, p. 7). Following threat identification, risk management defines individual component deliverable levels (HB 167, 2006, p. 69; Talbot & Jakeman, 2009, p. 11), achieving a threat driven risk based systems approach. The next stage considers the practice of demarcating and dividing space into zones of protection (Williams, 1981, p. 143; SAND Institute, 2002, p. 5) referred to as compartmentalizing (Bintliff, 1992, p. 130). This practice also considers employing crime prevention through environmental design (CPTED) as design inputs into the system, underpinned by the overlapping strategies of natural access control, natural surveillance and territorial reinforcement (Crowe, 2000, pp. 1-36).

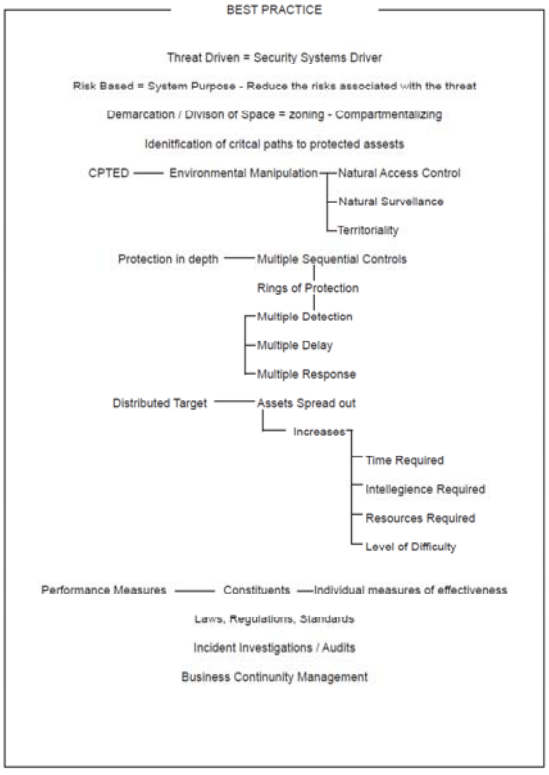

Figure 3. A preliminary conceptual map of cross referenced security category knowledge domains

Best practice encompasses protection in depth, involving a number of distinct measures an adversary must defeat in sequence and considers the avoidance of single point failure in any protection plan (Williams, 1981, p. 143; American Institute of Architects, 2001, p. 11; Garcia, 2008, p. 6), considered the "rings of protection" (Higgins, 1989, p. 229). Protection incorporates multiple detection measures, multiple delay measures and multiple response capabilities and back-up systems (Williams, 1981, p. 143; Garcia, 2008, p. 6), to complement each other, overcome individual weaknesses and minimise the consequences of component failure (Garcia, 2008, pp. 5-6). This approach is supported by the practice of distributing the target within a protected environment (Garcia,

2001). Distribution increases the time required to penetrate all components, the intelligence required to successfully locate each asset and security controls, the resources required to compromise each asset and therefore, increasing the overall level of difficulty (Rational Choice).

Such an approach is supported by the setting of individual component performance measures (Garcia, 2008, p. 5) and applications of hierarchical- principles-combinations (Williams, 1981, pp. 145-147) across technical, procedural and physical controls. This functionally achieves the elements of defence in depth including intrusion detection and tamper detection, security lighting, access control, closed circuit television in what Bintliff (1992, p. 315) refers to as layered technology-based security, supported by physical delay constituents and response capabilities (See Williams, 1981, pp. 145-147; Bintliff, 1992. Fennelly, 1997; Konicek & Little, 1997; Cieszynski, 2001; Garcia, 2001; 2008; IESNA G-1-03 Security Lighting Comittee, 2003; Fisher & Green, 2004).

Such a system is considered, whilst being cognisant of the legal framework including relevant laws, regulations and standards, as guiding the implementation of individual protection components (Kovacich & Halibozek, 2006, pp. 37-46; Garcia, 2008, p. 5). Within this approach, the practice of investigating and analysing security related incidents supported in the writings of Astor (1978, pp.153-160), and consistent with the recovery element (HB 167, 2006, pp. 63-64; Australian Government, 2008, p. III) is holistically supported through robust business continuity management (Talbot & Jakeman, 2009, pp. 365-367).

Furthermore, for both teaching and learning purposes, it can be useful to represent visually the interrelationships between concepts. As such, concept maps (Figures 2 & 3) are graphically condensed (Figure 4) to represent a threat driven risk based design heuristic for security systems planning.

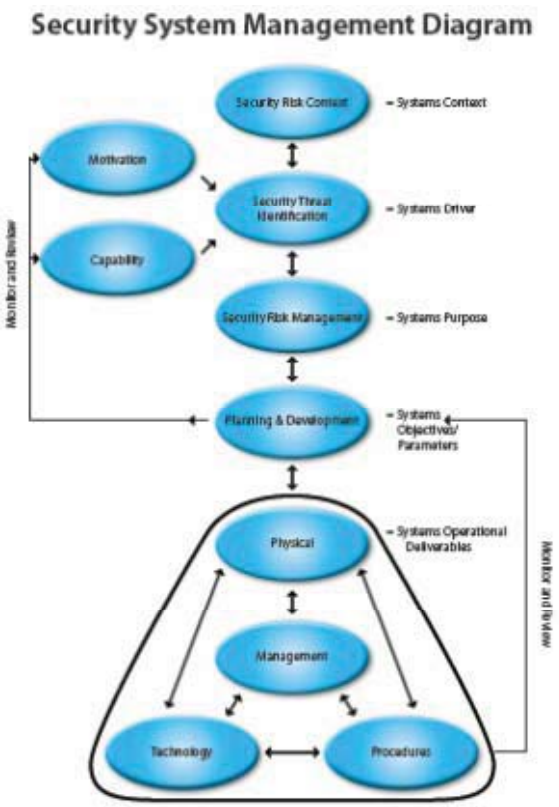

Figure 4. Threat driven risk based design philosophy for security systems

CONCLUSION

This paper presented phase one of a multiphase study. Results indicate that within a systems approach to security the core professional competencies for a security professional relate to their ability to skilfully apply knowledge from the theories and best practice principles embodied within the security domain planning and management heuristic. This heuristic was approached accordant with the works of Fraser (1993, p. 18), who pointed out that as a construction, knowledge is changeable as people revise their constructions of knowledge and incorporate new information in different ways into their existing conceptual frameworks. The heuristic map (Figure 2) takes

a top-down approach bounded by routine activity, rational choice, situational crime prevention, defence in depth, security decay, and management theories, within the elements of prevention, preparedness, response and recovery. It is argued this heuristic will enhance more meaningful learning within security science and bring together academic theory with practising security strategies. It is proposed that this heuristic will be adjusted throughout the remaining phases of the study; however, phase one supported the viability of further phases towards the development of a consensus heuristic for the security domain.

REFERENCES

Astor, S. D. (1978). *Loss prevention: controls and concepts*. Butterworth Publishers. Stoneham.

Australian Interim Security Professional's Task Force. (2008). Advancing security professionals: Discussion paper. Retrieved from August 2011: http://www.isaca-adelaide.org/pd/Discusion_paper_Future_Security_Professionals_March08.pdf.

Australian Government. (2008). National Counter-terrorism plan: National Counter-Terrorism Committee. Retrieved August 2011 from: http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/85A16ADB86A23AD1CA256FC600072E6B?OpenDocument

Ausubel, D. P., Novak, J., D., & Hanesian, H. (1968). *Educational psychology: A cognitive view* (2nd e.d.). New York: Holt, Rinehart and Winston.

Bedard, J. & Chi, M., T.H. (1992). Expertise. *Current Directions in Psychological Science,* 1, 135.

Bintliff, R. L. (1992). *The complete manual of corporate security and industrial security*. New Jersey: Prentice Hall.

Brooks, D. J. (2010). What is security: definition through knowledge categorisation. *Security Journal, 23*, 225–239. doi: 101057/sj.2008.18.

Borodzicz, E., & Gibson, S. D. (2006). Corporate security education: towards meeting the challenge. *Security Journal, 19*, 180-195.

Cieszynski, J. (2001). *Closed circuit television* (3rd e.d.). Burlington: Elseier.

Clarke, R. V. G. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*. *20*(2).

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: a Routine Activity Approach. *American Sociological Review*, 144: 588-608.

Cohn, B. M. (1981). Reconciling fire safety and security requirements for buildings. *Building Security, ASTM STP 729. American Society for Testing and Materials*.

Collins Australian Pocket Dictionary of English Language. (1994). Victoria: Harper Collins Publishers.

Cornford, I. & Athanasou. (1995). Industrial and commercial training. *Guilborough,* 27: 10-19.

Craighead, G. (2003). *High-rise security and fire life safety* (2nd e.d.). Woburn, MA: Butterworth-Heinemann.

Crowe, T. D. (2000). Crime prevention through environmental design (2nd e.d.).National Crime Prevention Institute. Boston: Butterworth-Heinemann.

Donald, A. S. (1983). *The reflective practitioner: How professionals think in action*. BasicBooks.

Eysenck, M., W. & Keane, M., . (2001). *Cognitive psychology: A student's handbook* (4th e.d). New York. Psychology Press.

Fennelly, I. J. (1997). *Effective physical security* (2nd e.d.). Boston: Elsevier Butterworth-Heinemann.

Fisher, R. J., & Green, G. (2004). *Introduction to Security* (7th e.d.). Boston: Butterworth- Heinemann.

Fraser, K., M. (1993). Theory based use of concept mapping in organisation development: Creating shared understanding as a basis for the cooperative design of work changes and changes in working relationships. UMI Dissertation Information Service. Michigan.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston: Butterworth-Heinemann.

Garcia, M. L. (2006). *Vulnerability Assessment of Physical Protection Systems*. Boston: Butterworth-Heinemann.

Higgins, C. E. (1989). *Utility security operations management: for gas, water, electric and nuclear utilities*. Illinois: Charles C Thomas Publisher.

IESNA G-1-03 Security Lighting Committee (2003). Guidelines for security lighting for people, property and public spaces. *Illuminating Engineering Society of North America.*

Konicek, J., & Little, K. (1997). *Security, ID systems and locks: The book on electronic access control*. New York: Butterworth-Heinemann.

Lussier, R., N. (2006). *Management fundamentals: concepts, applications and skill development* (3rd e.d.). Thomson South-Western. Mason.

Manunta, G. (1999). What is security? *Security Journal*.12, 57-66.

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

Sennewald, C. A. (2003). *Effective security management* (4th e.d.). Boston: Butterworth-Heinemann.

Standards Australia. (2006). *Security risk management.* Sydney: Standards Australia International Ltd.

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

Umibe, F. (1991). Technical management notes. *Transactions on Engineering Management*, 38 (4), 359-365.

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

Vu, T., Rigby, B., Wood, L. and Daly, A. (2011). Graduate skills in business learning. *Asian Social Science*, *7*(4): 2-12.

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

Williams, J. D. (1981). Design considerations for high-security interior intrusion detection systems. *Building Security, ASTM STP 729. American Society for Testing and Materials*.

Winoto, P. (2003). Controlling malevolent behaviour in open multi-agent systems by means of deterrence theory. *Proceedings of the IEEE/WIC international Conference on intelligent agent technology* (IAT'03).