2011

Security risk management: A psychometric map of expert knowledge structure

David Brooks
Edith Cowan University

10.1057/rm.2010.7
This article was originally published as: Brooks, D. J. (2011). Security risk management: A psychometric map of expert knowledge structure. Risk Management, 13(1-2), 17-41. *The final publication is available at link.springer.com via* https://doi.org/10.1057/rm.2010.7

Security risk management: A psychometric map of expert knowledge structure

David J. Brooks
Security Research Centre (secau)
Edith Cowan University
Email: d.brooks@ecu.edu.au

Abstract

The security industry operates within a diverse and multi-disciplined knowledge base, with risk management as a fundamental knowledge domain within security to mitigate its risks. Nevertheless, there has been limited research in understanding and mapping security expert knowledge structures within security risk management to consider if parts of security risk management are unique from more general risk management. This interpretive study applied a technique of multidimensional scaling (MDS) to develop and present a psychometric map within the knowledge domain of security risk management, validated with expert interviews.

The psychometric MDS security risk management concept map presented the expert knowledge structure of security risk management, demonstrating the inclusive and spatial locality of significant security risk concepts, conceptual complexity and uniqueness of the domain and the importance of the concept *threat*. Understanding security experts' consensual knowledge of security risk may allow improved understanding of threat-based risk, the issue with applying probabilistic risk analysis against antagonist events, and improved teaching and learning within this knowledge domain.

Key words: Security, risk management, knowledge structure, experts

Introduction

Over the past two decades, the concept of risk management as a formal discipline has emerged throughout the private and public sectors (Aven, 2008; Power, 2007). Risk management has now become a well established discipline, with its own body of knowledge and domain practitioners. States worldwide have their own risk management standards and in many of these states, it is the senior company executives who have responsibility to ensure that appropriate risk management practices meet internal and external compliance requirements (D. J Brooks, 2009a). Nevertheless, many of these standards and compliance requirements only consider risk management, not security risk management. Security risk management may be considered unique from other forms of risk management, as many of the more generic risk models lack key concepts necessary for effective design, application and mitigation of security risks.

In general, security may be considered assured freedom from poverty or want, precautions taken to ensure against theft, espionage, or a person or thing that secures or guarantees (Angus & Roberston, 1992). According to Fischer and Green (Fischer & Green, 2004, p. 21) "security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury." Security practice areas may be considered public security (state policing), private security, national security, private military security or many other terms, but convergence of these areas are increasing in the current social and political environment. As Zedner stated "scholars have tended to think about security within their immediate discipline and in detachment from one another" (2009, p. 3). Such diversity may result in a society that has no clear understanding of what security is, moreover, there is a divergence of interests from

many stakeholders (Manunta, 1999). Nevertheless, the security industry incorporates diverse, multi-disciplined and capricious practitioners, originating from many disciplines; however, security risk management is a core skill for these security practitioners (D.J. Brooks, 2009b), resulting in the importance of this type of study.

Background

World exposure to terrorist attacks in Mumbai (2009), Jakarta (2009; 2004), Glasgow (2007), London (2007; 2006; 2005), Russia (2004), Spain (2004), Bali (2002) and New York (2001) has raised social concern over the ability of governments to protection its citizens. The previous Australian Prime Minister, Mr. John Howard, stated that the 2002 Bali attacks had touched all Australians, resulting in Federal Government committing an additional A$3.1billion to deal with the terrorist threat. The financial impact of the 11th September 2001 cost the United States 0.75 percent of US GDP or US$75 billion (Howard, 2004). These issues have raised both national and international requirement for security that can effectively protect its citizen at a reasonable cost, achieved to some degree through the use of security risk management.

Within the context of this study, security was considered within a commercial, organisational or private context for the protection of people, information and assets. This view was supported by ASIS International (2000), when indicating that organisational security management is a distinct field, separate from police or justice domains. Otherwise, with the breadth of applied security domains, there could be a divergence of these distinct knowledge categories.

Over the past two decades, the concept of risk management has flourished throughout the private and public sectors (Aven, 2008; Power, 2007). Security, like other management disciplines, has embraced the principles and application of risk management, in particular, a probabilistic risk approach to measure risk and aid decision-making (Standards Australia, 2006; Talbot & Jakeman, 2008). Such an approach has been supported by many, who view probabilistic risk as a tool that produces rational, objective and informed options from which decisions may be made (Garlick, 2007; Morgan & Henrion, 1990; Talbot & Jakeman, 2008). However, many argue that probabilistic risk is inadequate for delivering (expected) rational measurements of security risks in what may be considered an increasingly uncertain and changing environment (Bier, 1999; Bier, 2007; L. A. Cox, 2008; Manunta, 2002).

Australia's approach to security risk management

There are a number of risk management and security risk management frameworks used by the Australian security industry including Australian Standard 4360:2004 Risk Management (Standards Australia, 2004a), Handbook 167:2006 Security Risk Management (Standards Australia, 2006) and the Risk Management Institute of Australasia Security Risk Management Body of Knowledge (SRMBOK) (Talbot & Jakeman, 2008). Australian Standard 4360:2004 has now been modified and used as the basis for the International Standards Organisation ISO3100:2009 for risk management.

AS ISO 3100:2009 Risk Management

AS4360 Risk Management (Standards Australia, 2004a) was first published in 1992 and is considered "almost a de facto global standard" (Jay, 2005, p. 2), becoming "recognised internationally as best practice" (Jones & Smith, 2005, p. 23) on dealing with risk, having been used in Canada and the United Kingdom, and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005, pp. 2-3). The standard is widely used by

security professionals within Australia (Jones & Smith, 2005, p. 23) and became the draft for the International Standards Organisation ISO 31000:2009 Risk Management (Standards Australia, 2009, p. vi). Many industries use this framework and it has broad application across governance, finance, engineering, project management, environmental protection, life safety and security.

Standards Australia is Australia's peak standards organisation, even though they are a public company limited by guarantee. Standards Australia is charged by the Australian Commonwealth Government to provide general oversight and governance of Australian Standards (Standards Australia, n.d.), with four key areas of focus including national and international coordination, accreditation of other organisations to produce standards, development and update of standards, and design assessment (Standards Australia, 2009).

Australian Standards, as with most standards, are "published documents setting out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform" (Standards Australia, n.d. p. 2). Such an approach ensures that a common *language* is achieved within an industry, driven by the more progressive parts of industry, legislation and community expectations.

AS ISO 31000:2009 Risk Management presents a framework (Figure 1) or process (Standards Australia, 2009, p. vi) for the risk management process, beginning with *establishing the context*, where the scope is set and stakeholders are identified. Next the risks are *assessed*, integrating risk *identification, analyses* and *evaluation*, and finally risks are *treated*. Concurrently with the risk assessment stages, the process is *monitored and reviewed* and stakeholders are *consulted* (Standards Australia, 2004b).

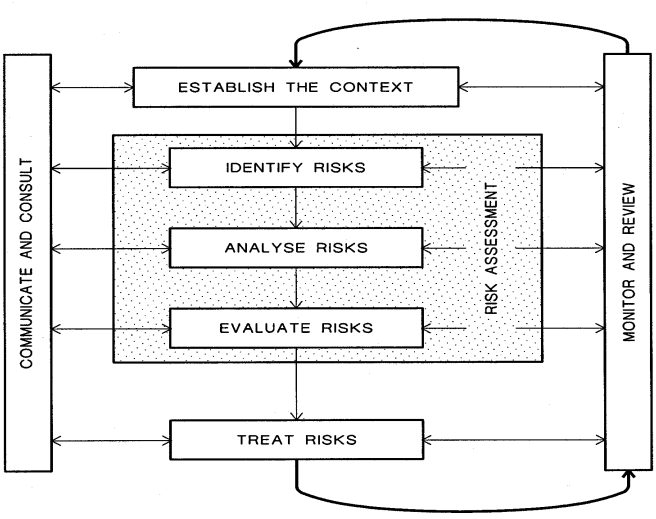

Figure 1. Risk management.
(Standards Australia, 2004b; Standards Australia, 2009)

What the AS ISO 31000:2009 Risk Management standard does not consider are security risk concepts such as *threat*, *vulnerability* and *criticality*, which could be considered significant. Such limitations were addressed by Standards Australia when they developed, in consultation with academia and the security industry, a specific security risk management standard, namely Handbook HB167:2006 Security Risk Management.

HB167:2006 Security Risk Management

As Standards Australia stated in their handbook of security risk management, "the field of security risk management is rapidly evolving and as such this Handbook cannot cover all aspects and variant approaches" (2004d, p. 2). As the security risk management concept map has demonstrated, *threat* is a critical factor when considering security risk. However, the Risk Management AS4360:2004 Standard does not present the concept of *threat* or other security related concepts such as *vulnerability*, even through Risk Management AS4360:2004 Standard is a primary resource for security practitioners when considering and applying security risk management.

HB167:2006 does "provide a means of better understanding the nature of security threats" (Standards Australia, 2006, p. 6). For example, the handbook considers such security risk concepts as *threat*, *criticality* and *vulnerability* (Figure 2); all significance and unique to this domain of risk management (D. J Brooks, 2009a).

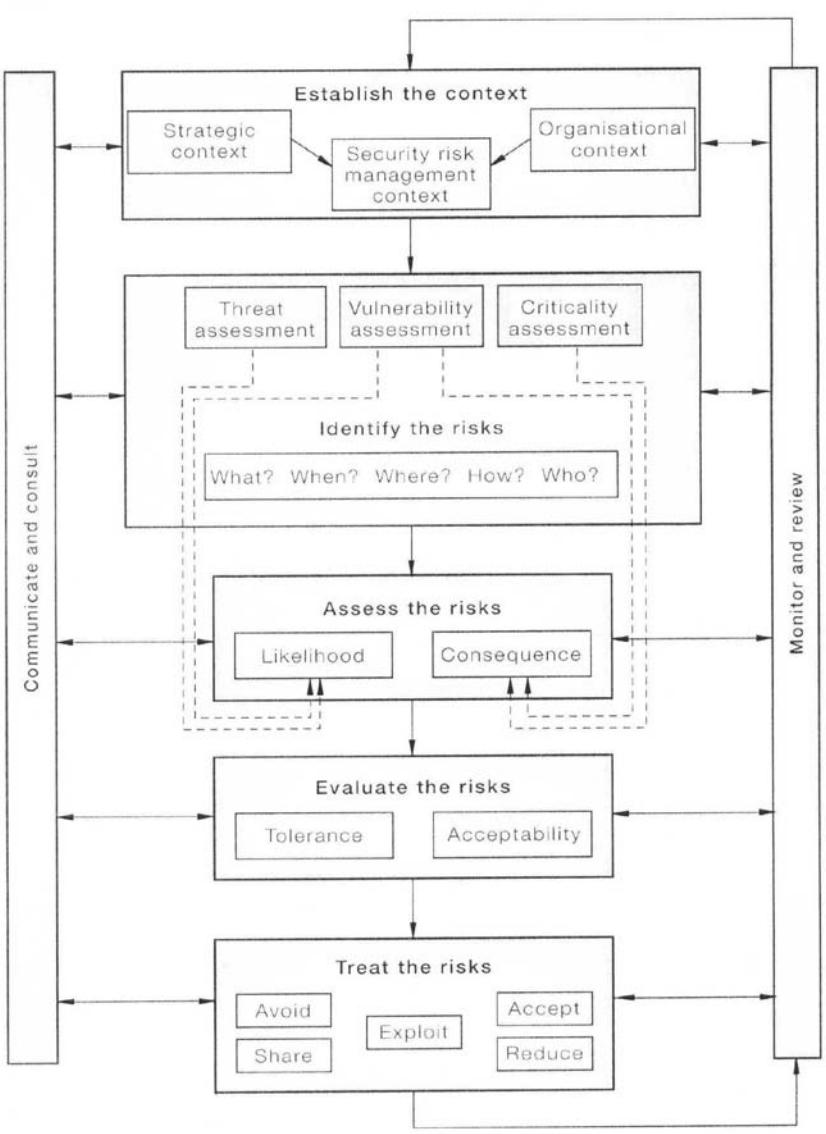

Figure 2. HB167:2006 Security risk management framework.
(Standards Australia, 2006, p. 14)

Other Security Related Australian Standards

Finally, within Standards Australia there are other specialised security risk related standards covering areas such as business continuity management, health, information security, outsourcing risk, finance and corporate governance (Table 1).

Table 1
Security related Australia Standards

Number	Title
AS4485.1:1997	Security in health care facilities
AS8000:2003	Corporate governance
AS ISO/IEC27001:2005	Information technology – Security requirements
HB141:1999	Risk financing guidelines
HB221:2003	Business continuity management
HB240:2000	Guidelines for managing risk in outsourcing
HB254:2005	Governance, risk management and control assurance

Whilst many of these frameworks have been developed in an attempt to account for risk (Aven, 2008; Garlick, 2007), security, like many management disciplines has embraced a probabilistic risk analysis approach (Manunta, 2002; Standards Australia, 2006; Talbot & Jakeman, 2008). Based on a quantitative, semi-quantitative or qualitative assessment of the probability and consequences of future events, probabilistic risk aims to provide security managers with a measurement of such risks. Measurements are then used to formulate cost-effective decisions to *shape* a future which (attempts to) minimise potential harm, whilst captialising on potential opportunities (Garlick, 2007). Nevertheless, it can be suggested that such a probabilistic approach does not provide risk management efficacy for security and security risk management has to take a greater heuristic approach.

Security Risk Management Body of Knowledge

A framework that to some degree takes such a heuristic approach is the Risk Management Institute of Australasia (RMIA) Security Risk Management Body of Knowledge (SRMBOK). The need to increase security risk management knowledge was shown through an Australian Federal Government supported initiative with the RMIA, resulting in the Security Risk Management Body of Knowledge (Talbot & Jakeman, 2008) guide for practitioners. The guide attempts to resolve security risk management elements such as “a framework for critical knowledge, competency and practice areas which managers, practitioners, students and academics alike can apply to recruit, train, educate and measure performance” (Risk Management Institute of Australasia, 2007b, p. 1). Nevertheless, the SRMBOK still does not present clear identification of the many components and their interrelationships that could be considered security risk management.

Significance of the study

The risk and security risk management frameworks presented provide a number of structures or processes that practitioners may apply; however, they do not provide an in-depth understanding of conceptual interrelationship between their parts. In addition, they do not address how practitioners may or may not understand such relationships and whether such frameworks are consensual in their approach. The psychometric MDS concept mapping technique allowed such an understanding to be gained in security risk management. This research allowed greater understanding of expert knowledge structure, improved security education and curriculum design, and better development of the unique risk domain of security risk management.

Study objectives

The study used a psychometric technique to present a consensual concept map of *security risk management,* with a number of discrete research questions, namely:

- What is the expert knowledge structure and subordinate concepts of security risk management, as measured by multidimensional scaling?
- What is the expert knowledge structure and subordinate concepts of security risk management, as measured by interviews?
- Can a psychometric multidimensional scaling concept map of the security risk management knowledge structure and subordinate be developed and presented?

A number of significant outcomes from the study were expected. These outcomes included a better understanding of the security risk management knowledge structure, with the more significant security risk management knowledge concepts tabulated. Once these more significant security risk management concepts were defined, a security risk management knowledge and concept map could be developed.

Theoretical framework

A number of discrete theories supported the interpretive approach applied within the study, including knowledge categorisation, concept mapping and multidimensional scaling (MDS). These theories provided the inquiry with a scientific foundation. Knowledge categorisation included cognitive memory, knowledge categorisation and expertise. Concept mapping and MDS supported the development of security knowledge categorisation and subordinate concept modelling.

Knowledge Categorisation

Knowledge may be considered as "facts or experiences known by a person or group of people, specific information about a subject" (Angus & Roberston, 1992, p. 557). However, according to Clancey, knowledge "is more than written scientific facts and theories" (1997, p. 285). Knowledge is not discovered, on the contrary, knowledge uses and expands existing concepts (Novak, J.D. & Gowin, 1984) and is "a possible state of affairs, either real or imaginary" (Eysenck & Keane, 2002, p. 533). As new knowledge is gained, change in understanding regarding existing knowledge is achieved. Knowledge is *viable* (Rennie & Gribble, 1999), constructed and is built on previous knowledge.

Knowledge is integral to memory structure – defined as the way in which memory is organised, stores and retrieves information. The memory process has a major impact on the ability of long term memory (LTM) to retain and retrieve (Eysenck & Keane, 2002) and is a complex interactive process (Lockhart & Craik, 1990), which requires knowledge categorisation. A person is exposed to information in their everyday life and concurrently knowledge has to be economised and abstracted into categories, generally referred to as *concepts*. Concepts may be further divided into implicit (inclusive) or explicit (concrete) concepts. These concepts are developed and maintained within long-term memory, however there is a cognitive balance between the number and effectiveness of possible concepts. Concepts need to be *informative*, based to a degree on the natural world, economic and cohesive (Eysenck & Keane, 2002) and organised into categories (Kellogg, 2003). Similar objects are grouped together within a conceptual category and these groupings are generally a product of the learner's environment. There are four theories for concept categorisation, being the *defining-attribute*, *prototype*, *explanation* and *exemplar-based* views (Eysenck &

Keane, 2002). The exemplar based view was considered the informing theory supporting knowledge categorisation.

Concept Mapping

Concept maps may be defined as a representation of a state of affair or situation. People may attempt to understand the world though developing a concept map of the situation, an idea, understanding or principle. Concept maps are thinking tools, that are used to explore different aspects of a topic (Wallace, Schirato, & Bright, 1999). Concept maps are generally imaged, dynamic and outcome-based simulations that are used in everyday life to think and understand the world (Eysenck & Keane, 2002; Johnson-Laird, 1983; Norman, 1983). Concept maps enable people to exchange an idea, have shared understanding, provide a common language, reach conclusions in decision-making and guide their action (Norman, 1983; Novak, J.D. & Gowin, 1984). Concept maps may also be referred to as *mental maps*, *mind maps*, *naive theories* or *folk theories*, although these are considered to have different characteristics (Bennett & Rolheiser, 2001).

Concept maps attempt to present many aspects of human cognition, from direct representation of a physical entity to abstract thought. This view supports concept understanding as once a person understands the physical process, most will accept a formal model of the process (Bar & Travis, 1991). Representation of abstract thought is far less defined and involves implicit knowledge, although these models will "represent aspects of external reality" (Borges & Gilbert, 1999, p. 96). According to Eysenck and Keane (2002), people will often make discoveries using concept models to simulate aspects of the world, an ability that appears to depend on domain specific knowledge based on experience.

Concept maps may take many forms, however within the context of this study they are defined as graphical representations of structured knowledge. According to Novak and Gowin, concept maps are a "schematic device for representing a set of concept meanings embedded in a framework of propositions" (1984, p. 15). The schema may be as a body of knowledge, being the summation of domain experts understanding of their knowledge structure at that point in time (Trochim, 2005b), or as an individual and how a concept map may represent their understanding. Experts tend to define their knowledge within concept clusters, which are more extensive, have greater cross concept linkage, increased branches, greater hierarchical structure and are more complex (Markham, Mintzes, & Jones, 1994).

There are many methods to develop concept maps, with an enormity of variations that may extract, develop and represent concept maps (Ruiz-Primo, Schultz, Li, & Shavelson, 2001). According to Johnson-Laird (1983), concept maps may be divided into two distinct types, namely *physical* or *conceptual* maps. Physical maps provide representation of physical systems and research has tended to focus on physical objects, particularly in chemistry, physics and biology domains (Johnson-Laird, 1983; J. D. Novak, 1998), whereas conceptual maps represent abstract or inclusive knowledge categorisation (Eysenck & Keane, 2002; Reisberg, 2001). The study used both quantitative and qualitative techniques to extract and present a conceptual psychometric concept map of security risk management.

Multidimensional Scaling

Multidimensional scaling (MDS) is a statistical technique within the area of multivariate analysis. MDS reduces complex *n*-dimensional data and represents these data within a spatial format. The reduction in data complexity through presentation in *n*-dimensional space allows hidden data structure formation — demonstrating object proximity — with *proximity* being

how similar or dissimilar objects are perceived to be (T. F. Cox & Cox, 2000; Kruskal & Wish, 1978). MDS commences with a set of objects, which are paired and their similarities measured. The distance between pairs of objects are placed into a half matrix format. Configurations of points are sought in *n*-dimensional space, with each point representing an object. MDS calculates *n*-dimensional space configuration where the points distance *match* the paired dissimilarities. The variation in *matching* defines the different techniques of MDS (T. F. Cox & Cox, 2000), with the study using the ALSCAL algorithm:

$$\delta re = \left\{ \sum_{i} \quad (\mathcal{X}ri - \mathcal{X}si) \quad ^{2} \right\}^{½}$$

MDS provided a suitable tool (Smith, 2003) to categorise knowledge concept clusters within *n* dimensions. This method is supported by Ohanian (cited in Stein, 1997), whom stated that expertise can be measured as a construct that contains multiple dimensions. MDS facilitated the construction of the security *consensual* map. MDS produced a spatial representation of knowledge concept clusters, allowing an analysis of judgements between variables to define dimensionality between such variables (Cohen, Manion, & Morrison, 2002). MDS also provides a moderate to good construct validity for concept mapping (Hoz, Bowman, & Chacham, 1997, p. 928).

The use of MDS in concept mapping was first presented by Trochim (1989b), with later work that expanded and detailed the methodology of constructing and presenting concept maps (Trochim & Cook, 1994). Nevertheless, Trochim's (1989b) earlier work considered only knowledge structure, a rather restricted approach that contradicted the view of concept mapping (1990) and which continued to more recent work (Trochim, 2005b). During this period Markham, et al. (1994) used MDS as a method to test the validity of concept mapping, considering the previous work by Novak (1990). Markham, et al. (1994) demonstrated that concept mapping provided a theoretically valid and powerful tool, and that MDS proved an appropriate statistical technique to define concept maps. A view that more recent researchers have validated, through additional MDS concept mapping studies (Ruiz-Primo et al., 2001; Streveler, Miller, & Boyd, 2001).

Published literature have integrated both concept mapping and MDS, which included studies that considered a scientific method to design a teaching methodology used in basic signal processing (Martinez-Torres, Garcia, Marin, & Vazquez, 2005), the spatial variation of species diversity (Cheng, 2004), techniques used by physiotherapists in Southeast Australia (Turner, 2002) and computer-based collaborative learning environments (Kealy, 2001). These studies have lead to the general conclusion that psychometric MDS concept mapping presents valid and robust concept maps.

Study design

The study was divided into three distinct phases (Table 2), designed to respond to the three research questions.

Table 2
Study design

Phase	Description	Outcome
One	Knowledge categorisation	Extracted list of security risk concepts

Two	MDS knowledge structure	Knowledge structure of security risk
Three	Expert knowledge structure validation	Concept map of security risk

Phase one: Knowledge categorisation

The study commenced with Phase one and knowledge categorisation, where 104 English speaking institutions that offered tertiary security courses at undergraduate or postgraduate level were investigated and critiqued. Search methods to identify these courses used the world-wide-web, ASIS International (2007), Security Institute (Kidd, 2006), Australian University Guide (Good Guides, 2004) and Association of Universities and Colleges of Canada (2005). There was no limitation placed on the search criteria, as all institutions that offered security and allied industry courses were assessed (Table 3). In the world-wide-web search engines, typical data strings used were *security; security course; security management.*

Table 3
Location and number of security related courses

Country of origin	Institutions offering security related courses
Australia	11
Canada	8
United Kingdom	5
United States of America	74
New Zealand	5
South Africa	1
Total	104

Initial course selection was based on course title, supported by three industry and academic security experts. Further analysis reduced the number of courses to seven for content analysis. Once the final seven courses were selected for content analysis, course syllabi were sourced. Course syllabi included the course overview, and unit of study descriptions, objectives and content overview. Concept extraction commenced with an initial analysis of each critiqued course. Course structures were analysed for security and risk concepts, extracted using Linguistic Inquiry and Word Count (LIWC) text and content analysis (Pennebaker, Francis, & Booth, 2001). Course transcripts were sanitised, as generic study or research skills were not considered within the content analysis.

Initial analysis resulted in 56 security risk concepts being extracted; however, the most used security risk concepts were required for knowledge mapping. Therefore, further analysis was undertaken and considered such aspects as word frequency, context and locality. In addition, convergence was applied using the Australian Risk Management Standard AS4360:2004 (Standards Australia, 2004a), now ISO 3100:2009. Analysis resulted in a final *security risk management* category, with supporting subordinate concepts (Table 4).

Table 4
Risk management category and subordinate concepts

Security risk management		
Analysis	Assessment	Calculate
Communication	Consequence	Culture
Decision	Evaluation	Loss
Risk management	Perception	Probability

Risk	Threat

Phase two: Multidimensional scaling knowledge structure

The second phase developed the multidimensional scaling (MDS) psychometric knowledge map of the security risk experts. To achieve this outcome, a number of steps were taken to analyse and present the security risk management knowledge map (Figure 3).

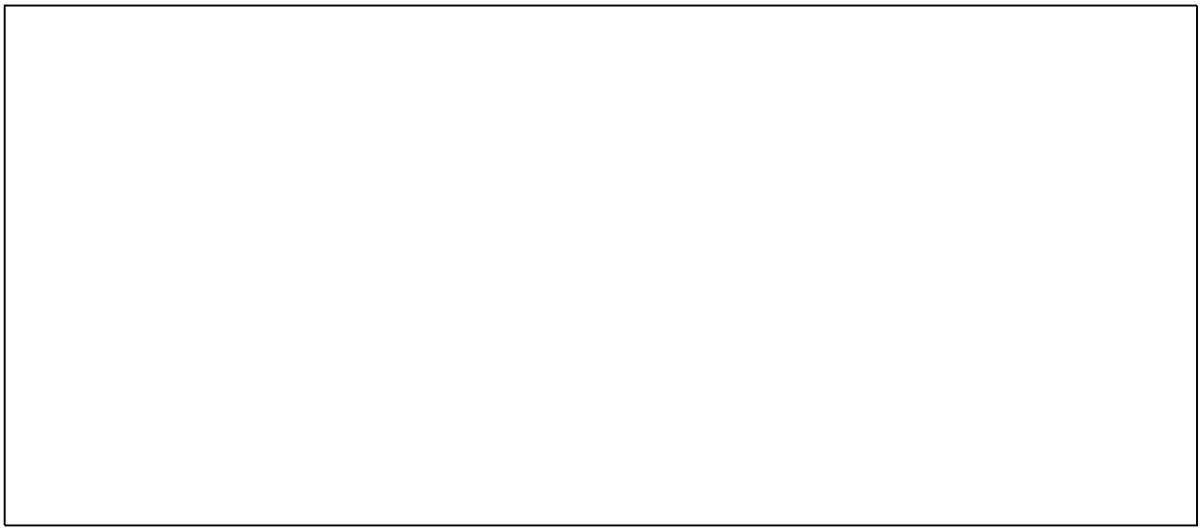

Figure 3. Psychometric MDS concept mapping methodology

Phase one data was inserted into the study's survey instrument (see Figure 4 for a sample), embedded with the 14 security knowledge categories (Table 3). Participants selected, on a sliding scale, how similar or dissimilar they considered pairs of these security risk concepts. Non-probabilistic selected expert participants (N=29) made up the study's sampling group. The sample size was selected to reduce the MDS STRESS1 measure (Cheng, 2004, p. 340; Cohen et al., 2002), but not exceeded due to the non-probability sampling method applied to expert selection.

when compared to			Similar	1	2	3	4	5	6	7	8	9	10	Dissimilar
Analysis		Assessment												
Analysis		Calculate												
Analysis		Communication												
Analysis		Consequence												
Analysis		Culture												
etc		etc												

Figure 4. Example of the MDS survey instrument

The security risk management experts were selected by non-probability sampling and based on the study's definition of expertise. As people gain domain knowledge, they may become more expert. Nevertheless expertise is not the exclusive gathering of information, moreover a rich understanding of knowledge, how that knowledge integrates into concepts and experience (Kellogg, 2003). Experts, unlike novice learners, understand domain knowledge in a hierarchical manner and have a more complex schema. This knowledge categorisation can be represented with concept maps, showing rich knowledge structure (Markham et al., 1994).

For the study an initial number of Australian experts were sourced, based on their known standing in the security risk management community. Each expert was asked to recommend additional leading security risk management practitioners or academics. From the peer recommendations, these additional experts were contacted until the proposed study sampling size was attained. On contact, each expert was given a synopsis of the study and requested that they participate in the MDS concept mapping survey. The MDS survey was administered to the experts via a number of methods, dependant on geographical location of the expert from the researcher.

Data was extracted from the sum of the experts' MDS survey instrument responses (Cronbach's Alpha α0.93), converted into a half-matrix and analysed using MDS. MDS ALSCAL analysis (STRESS1=0.28, RSQ=0.64) produced the spatial map (Figure 5), which required rotation and insertion of propositional statements.

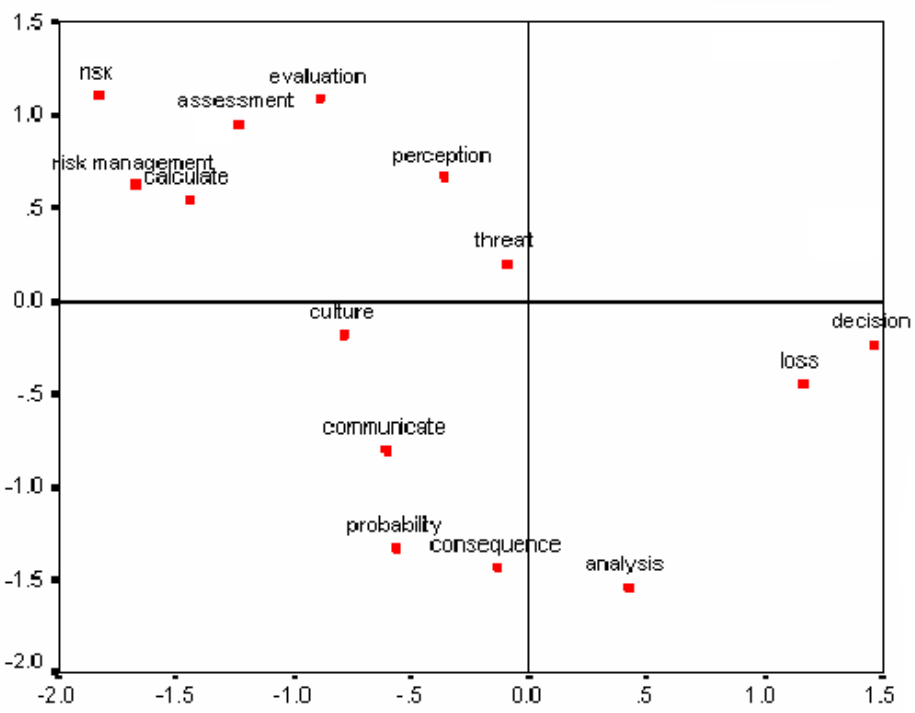

Figure 5. Psychometric security risk management knowledge structure
Notes: (comms = communications; cultrisk = cultural risk; intell = intelligence; psycho = perception; stats = statistics)

The psychometric security risk structure (Figure 5) had both dimensional x and y axis data removed, leaving only knowledge structure (Figure 6). The structure was also rotated approximately 35°, locating the concept *risk* upper most as the most implicit concept.

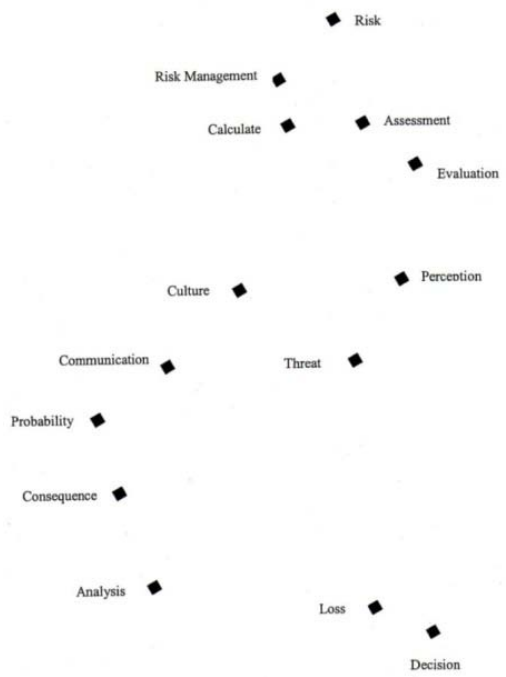

Figure 6. MDS concept knowledge structure ready for propositional linkage insertion

At this point, the MDS knowledge structure (Figure 6) was presented to experts (N=5) using a Delphi method. Each expert inserted propositional concept map links and labels in isolation to each other. Once this initial process was completed, the sum of the experts' results was compared and only *consensual* links and labels retained. The process was then repeated until any subsequent changes were minimal or not supported by a consensus. Such a process led to the *draft security risk management map*, which was further validated in the following Phase three.

Phase three: Expert knowledge structure validation

Phase three used expert interviews (N=6) to assess the validity of the *draft security risk management map*. An expert interview survey instrument was developed to analyse and interpret the opinions of the experts regarding such aspects as the security risk map structure, inclusivity of security risk concepts and concept propositions. To complete the study, a comparative stage to triangulate (Cohen et al., 2002, pp. 112-115) between Phase one and Phase two outcomes followed, where the appropriateness of the MDS security risk management consensual map (Figure 7) was considered.

Psychometric map of security risk management

The study presented the psychometric security risk management map (Figure 7), which resulted in a number of interesting interpretations. Such interpretations included the central locality of the concept *threat*, the clustering of psychology risk concepts to threat, the outlying of risk assessment concepts such as probability and consequence, and the experts' view that security risk management provided a quantitative analysis.

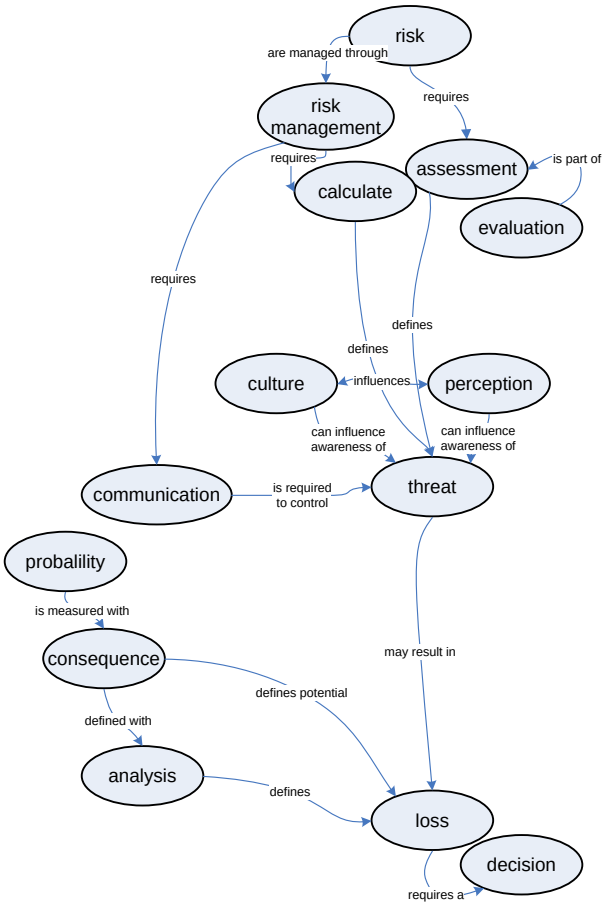

Figure 7. Psychometric security risk management concept map

The psychometric security map presented *threat* at the spatial centre of the map, indicating that this concept is most related to the other measured concepts; a locality that was strongly supported by the Phase three experts. As one of the experts stated, “if there is no threat then there is no risk”, supported by another who proposed that “threat is a fundamental that drives [security] risk”. Such locality raised a number of issues, one being that for many years AS4360 risk management standard was the primary source for security practitioners and threat is not considered in this standard. Nevertheless, this issue has been addressed in 2006 with the introduction of the Security Risk Management HB167:2006 handbook (Standards Australia, 2006).

According to the map, threat also has a close relationship to both *perception* and *culture*. Such relationship considers that to some degree organisational background will define the level of perception to threat based on the cultural acceptability. In other words, that both perception and culture informs the level of threat that an individual, organisation, community or society will be willing to accept or not. As McGill, et al., states, “the threat component … is arguably the most uncertain aspect of the security risk problem” (2007, p. 1266), requiring subjective assumptions to forecast the intentions of potential adversaries. If threat is so uncertain, then its drivers of perception and cultural further complicates this issue.

Many of the security risk management frameworks put forward in the introduction included the concepts of *probability* and *consequence* (Standards Australia, 2004a; Standards Australia, 2006). However, the security risk map presented these two concepts as relative outliers and not where one may expect these concepts to be located. A number of the

interviewed experts' did raise this issue and suggested that these two concepts should be closer to *analysis*. The concept cluster of *risk management*, *calculate*, *assessment* and *evaluation* appears to indicate that the experts' viewed security risk management as providing a quantitative or probabilistic analysis. Nevertheless, the participating experts all agreed that in general the two concepts of probability and consequence were suitably located. It may be suggested that experts' consider the importance of threat and have some implicit understanding that these concepts cannot necessarily provide a wholly suitable measure. Cox suggests that by taking such a probabilities approach to assessing the action of intelligent antagonist may lead to errors in risk estimates (L. A. Cox, 2008, p. 1749).

The study appeared to demonstrate a number of significant findings. These supported the research questions, with evidence to suggest that for the security risk management category:

- MDS represented an appropriate technique to provide structure in the foundation of consensual knowledge maps.
- Within the psychometric security risk map, the spatial localities of concepts provided an indication of conceptual interrelationships and relationships.
- An appropriate consensual psychometric map of the security risk category and supporting subordinate concepts was presented (Figure 7).

The security risk map structure, spatial representation and inclusion of the more significant security risk concepts provided evidence that the *psychometric security risk management* map appeared to represent an appropriate knowledge structure for the security category of *risk management*, strongly supported by the participating security experts.

Recommendations

The study outcomes lead to a series of recommendations in how the psychometric security risk management map informs understanding of security risk management and directs further inquiry. These recommendations suggest how the psychometric security risk management concept map may benefit both academia and professional understanding of security risk management including a greater understanding of expert knowledge structure, assist in developing a security body of knowledge, improved security directed pedagogy, better development of the unique risk domain of security risk management and security risk management application

Benefit of the psychometric security risk management concept map

Security lacks definition (Tate, 1997) and yet is a distinct field of practice and study (ASIS International, 2003b; D.J. Brooks, 2009b). Supported by professional security bodies such as Risk Management Institute of Australasia (RMIA) (Talbot & Jakeman, 2008) and ASIS International (2009), security risk management is a unique knowledge category of security. Nevertheless, the security industry is a diverse and a 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).

Risk management, as proposed by AS ISO 3100:2009, has been the primary methodological approach for security practitioners. In the past, the predecessor of AS ISO 31000:2009 was often considered "almost a de facto global standard" (Jay, 2005, p. 2) and has become an international template on dealing with risk. AS4360:2004 was used in diverse disciplines,

from finance to engineering and is used extensively by security and risk professionals across Australia (Beard & Brooks, 2006, p. 5; Jones & Smith, 2005, p. 2).

As Standards Australia suggested in their handbook of security risk management, "the field of security risk management is rapidly evolving and as such this Handbook cannot cover all aspects and variant approaches" (2004d, p. 2). As the security risk management concept map has demonstrated, *threat* is a critical factor when considering security risk; however, AS ISO 31000:2009 does not present the concept of *threat* or other security related concepts like *vulnerability*, even through this standard still remains a primary resource for security practitioners when considering and applying security risk management.

The need to increase knowledge of security risk management can be shown through an Australian Federal Government supported initiative with the RMIA. These groups, among others, developed and in 2007 published the Security Risk Management Body of Knowledge SRBOK) guide for practitioners. The guide attempts to resolve security risk management elements such as "a framework for critical knowledge, competency and practice areas which managers, practitioners, students and academics alike can apply to recruit, train, educate and measure performance" (Risk Management Institute of Australasia, 2007b, p. 1).

Most corporate security courses have been developed from related disciplines, being police, justice or criminology studies (Smith, 2001b; Tate, 1997), even through according to ASIS these disciplines should be separate and discrete from security (2003a, p. 4). At the tertiary level there is a lack of academic security programs, with most focused on criminal justice, crime prevention or risk management (Jay, 2005; Manunta, 1996, p. 235). This distortion of the corporate security discipline will result in security research that is not necessarily appropriate for the security industry. Security "is not merely a matter of intuition or common sense: it involves a complex body of knowledge, analytical abilities and know-how" (Simonsen, 1996, p. 229).

Nevertheless, according to Smith, security knowledge is being established though the development of appropriate domain concepts (2001a, p. 32), which is supported by Simonsen who stated that the "body of knowledge of security has grown rapidly in the past decade" (1996, p. 230). Security risk management is one such knowledge category that is core to the corporate security discipline (D.J. Brooks, 2009b). The security risk management concept map provides a degree of specialised security body of knowledge. Understanding the risk and security risk management concepts that security experts consider when assessing security risk, how these concepts relate and integrate, and why security experts consider these ideas all support understanding.

Further research

The study has lead to the need for greater research in certain aspects of security risk management. It is important to further validate the importance of the concept *threat* within security risk management. For example, is this concept the core driver when completing security risk management, as opposed to more general risk management?

The study used and measured the concept *probability*, as opposed to *likelihood*. The rationale behind the use of probability over likelihood was driven by the study's methodology in Phases one and two i.e., probability was a more used concept. Nevertheless, some view likelihood (Standards Australia, 2004d) as being a more relevant concept for security risk management due to greater qualitative cogitation. Further measurement of the relationship

between these two concepts would be appropriate. In addition, the importance of *vulnerability* needs to be considered.

The conceptual relationships put forward by the Australian Handbook (Standards Australia, 2004c) and RMIA (Talbot & Jakeman, 2008) for Threat Assessment, Vulnerability Assessment and Criticality Assessment requires greater understanding. As this study has put forward, threat is a central and core concept for security risk management. Does this add greater weight in important to Threat Assessments, what is more or less important when considering security risk management and when considering Criticality Assessment, is criticality better understood and therefore managed as this may better relate to security consequence?

Finally, the ability to validate the psychometric security risk management map needs to consider the study limitations. Further research could address this study's limitations through aspects such as a greater sample size or by applying a different methodological approach.

Methodological implications

Methodological limitations of the study were identified and included the ability to provide a conclusive definition of security, missing concept of *vulnerability*, sample size and extracted data, the ability of multidimensional scaling (MDS) to develop cognitive knowledge structure, and the reliability and validity of the study.

Defining security and its concepts

A total of 104 tertiary security courses were selected and validated by security experts; however, security has no clear definition (Horvath, 2004; Manunta, 1999; Tate, 1997) and "means different things to different people" (Davidson, 2005, p. 73). According to Hesse and Smith, security is diverse, without a defined knowledge or skill structure (2001, p. 89). A view put forward by Brooks, who suggest that security can only be defined through contextual understanding (D.J. Brooks, 2009b). Therefore, homogeneity in the selection and validation of expert groups within the study may have introduced some degree of distortion. To address this concern independent resources were used for data triangulation, for example the ASIS International Academic/Practitioner Symposiums (ASIS International, 2003b; ASIS International, 2009).

In considering the security risk management category, an additional subordinate concept of *vulnerability* could have been included in the psychometric map. Expert opinion indicated that this concept was a relatively important idea within security risk management. Such a view could also be suggested for the concept *likelihood*. Nevertheless, during study Phase one this concept was not identified and resulted in its exclusion. Therefore, the security risk management concept map has to be considered in the context of the homogeneity of the critiqued courses and expert validation groups.

Sample size and course nature

The study critiqued 104 tertiary security courses, resulting in a final analysis of seven courses. Since this critique there has been an increase in security undergraduate course offerings, with a claim that in the United States there are now "more than 300 two and four-year institutions that participate with homeland security programs" (Davidson, 2005, p. 72). However, it could be argued that these may not necessarily be appropriate organisational security undergraduate courses.

For greater statistical confidence, the sample study size could have been larger. In addition, due to the non-probabilistic sampling approach, homogeneity of study participants and experts could have been experienced. Both factors may have resulted in some degree of error in the psychometric security risk management concept map. But in another MDS concept mapping study on reliability (Trochim, 1993) an average of 14.62 participants were used, with the conclusion that MDS "sample sizes half as large are nearly as good as the full-size values, suggesting that even smaller samples … may produce maps that fit almost as well as samples twice as large" (Trochim, 1993, p. 11). Therefore based on the supporting MDS knowledge mapping evidence and with the need to gain an appropriately valid MDS sample size, in general the sample sizes were considered appropriate. Nevertheless, conclusions made have to be considered within the context of the sample size, nature of non-probabilistic sampling and homogeneity.

Cognitive knowledge structuring

The study has demonstrated that an appropriate expert knowledge structure of security risk management can be presented; however, knowledge is dynamic, complex and implicit (Lockhart & Craik, 1990; Rennie & Gribble, 1999). Exemplar knowledge categorisation, indicates that concepts have relationship attributes based on similarity (Cohen et al., 2002, pp. 294-295). Nevertheless, the ability of proximal data to represent knowledge structure has been criticised, both in its ability to represent cognitive structure and to provide useful pedagogy information (Smith, 1984, p. 254).

Reliability and validity of MDS concept mapping

Reliability and validity were considered throughout the study, cognizant of the relatively *high* MDS goodness-of-fit (STRESS1) measure, although Cronbach's Alpha reliability (α0.93), face and concurrent validity, and study triangulation all proved robust. MDS STRESS1 is a suitable MDS concept mapping measure — if a map achieved a value of less than 0.1 (Johnson & Wichern, 2002, p. 702) — of both reliability and validity. However this study, achieved what Johnson and Wichern would consider an inappropriately *high* STRESS1 (STRESS1=0.28, RSQ=0.64) measure. Nevertheless, this measure replicated findings of a similar larger MDS concept study (Trochim, 1993). In addition, Kealy (2001, p. 338) presented even higher STRESS1 results (STRESS1=0.36 to 0.35), with many other relevant MDS concept mapping studies not reporting their MDS goodness-of-fit measures (Lockhart & Craik, 1990; Markham et al., 1994; Martinez-Torres et al., 2005). Therefore, this study's STRESS1 was considered suitable, support from comparable MDS concept mapping studies.

Conclusion

Risk management and security risk management have flourished over the past decade and are relied upon to provide robust and informed mitigation strategies to protect people, information and assets. However, most risk management standards provide a framework or process that takes a probabilistic approach to risk management, perhaps not wholly suitable for security. This article has presented many of the Australian approaches to risk and security risk management, such as the ISO 31000:2009 risk management standard, Handbook AS436:2006 and the RMIA SRMBOK. Nevertheless, these frameworks or processes do not necessarily provide an in-depth understanding to security risk management and its uniqueness from risk management.

Using an interpretive approach with the foundation theories of knowledge categorisation, concept mapping and multidimensional scaling (MDS), this study has presented an experts' consensual psychometric map of security risk management. The study was divided into three

distinct phases, each informing the proceeding phase. The first phase critiqued 104 security courses and from these, tabulated the most subordinate security risk management concepts (N=14). These concepts were embedded into the MDS instrument to produce the spatial psychometric knowledge structure of security risk management, from which the final security risk management concept map was developed.

The psychometric security risk management map (Figure 7) presented a number of interesting aspects, such as the central locality of *threat*, the clustering of psychology risk concepts and the interrelationship of probabilistic analysis to security risk management. Threat was fundamental to security risk management, driven by an individual's perception and the organisational culture. Probability, consequence and analysis were clustered together and remote from the other general risk concepts, indicating that such a quantitative or probabilistic approach to security risk management may not be wholly suitable.

The psychometric security risk management map was developed and tested at every stage of the study, with indications that it was both reliable and valid. Such a map will benefit academia and industry understanding of security risk management, leading to improved frameworks, processes, teaching and learning. The map has shown the uniqueness of security risk management to risk management and augmented implicit understanding of experts in this complex risk domain.

Reference list

American Society for Industrial Security. (2000). *Proceedings of the 2000 academic/practitioner symposium*. The University of Oklahoma, Oklahoma: American Society for Industrial Security.

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

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

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

ASIS International. (2007). Academic institutions offering degrees and/or courses in security. Retrieved 7 March, 2007, from http://www.asisonline.org/education/universityPrograms/traditionalprograms.pdf

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

Association of Universities and Colleges of Canada. (2005). Speaking for Canada's universities at home and abroad. Retrieved 28 July 2005, 2005, from http://oraweb.aucc.ca/pls/dcu/

Aven, T. (2008). *Risk analysis: Assessing uncertainties beyond expected values and probabilities*. West Sussex: John Wiley & Sons Inc.

Bar, V., & Travis, A. S. (1991). Children's views concerning phase changes. *Journal of Research in Science Teaching, 28*(4), 363-382.

Beard, B., & Brooks, D. J. (2006). Security risk assessment: Group approach to a consensual outcome. *Proceeding of the 7th Australian Information Warfare and Security Conference*, 5-8.

Bennett, B., & Rolheiser, C. (2001). *Beyond Monet: The artful science of instructional integration*. Toronto: Bookation Inc.

Bier, V. M. (1999). Challenges to the acceptance of probabilistic risk analysis [Electronic version]. *Risk Analysis, 19*(4), 703-710.

Bier, V. M. (2007). Choosing What to Protect [Electronic version]. *Risk Analysis, 27*(3), 607-620.
Borges, T. A., & Gilbert, J. K. (1999). Mental models of electricity. *International Journal of Science Education, 21*(1), 95-117.
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.
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. ed.). London: RoutledgeFalmer.
Cox, L. A. (2008). Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks [Electronic version]. *Risk Analysis, 28*(6), 1749-1761.
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.
Davidson, M., A. (2005). A matter of degrees. *Security Management, 49*(12), 72-99.
Eysenck, M. W., & Keane, M. T. (2002). *Cognitive psychology: A student's handbook* (4th ed.). New York: Psychology Press Ltd.
Fischer, R. J., & Green, G. (2004). *Introduction to security* (7th ed.). Boston: Butterworth Heinemann.
Garlick, A. (2007). *Estimating risk: a management approach*. Aldershot: Gower Publishing Company.
Good Guides. (2004). Helping you make decisions about where and what to study in Australia. Retrieved 28 October 2004, 2004, from http://www.thegoodguides.com.au/ggcontent/course/id
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.
Horvath, J. (2004). The fear factor. Retrieved 3 September 2004, 3 September 2004, from http://www.telepolis.de/english/inhalt/te/18187/1.html
Howard, J. (2004). Business government forum on national security. Retrieved 3 July 2004, 3 July 2004, from http://www.safeguardingaustralia.org.au/Questions/Howard-address-23June04.doc
Hoz, R., Bowman, D., & Chacham, T. (1997). Psychometric and edumetric validity of dimensions of geomorphological knowledge which are trapped by concept mapping. *Journal of Research in Science Teaching, 34*(9), 925-947.
Jay, C. (2005, 2005, 17 March). Big debacles help shape a new science. *The Australian Financial Review*, p. p. 2,
Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference and consciousness*. Cambridge: Cambridge University Press.
Johnson, R. A., & Wichern, D. W. (2002). *Applied multivariate statistical analysis* (5th ed. ed.). Upper Saddle River: Prentice Hall.
Jones, D. E. L., & Smith, C. L. (2005). The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management. *Recent Advances in Counter-Terrorism Technology and Infrastructure Protection*.

Kealy, W. A. (2001). Knowledge maps and their use in computer-based collaborative learning environments. *Journal of Computing Research, 25*(3), 325-349.
Kellogg, R. T. (2003). *Cognitive psychology* (2nd ed. ed.). Thousand Oaks: Sage Publications.
Kidd, S. (2006). The Security Institute yearbook and directory of qualifications 2006. Retrieved 25 June 2007, 2007, from http//www.security-institute.org/yearbook.html
Kruskal, J. B., & Wish, M. (1978). *Multidimensional scaling* (Vol. 07). London: Sage Publications.
Lockhart, R. S., & Craik, F. I. M. (1990). Levels of processing: A retrospective commentary on a framework for memory research. *Canadian Journal of Psychology, 44*, 87-112.
Manunta, G. (1996). The case against: Private security is not a profession. *International Journal of Risk, Security and Crime Prevention., 1*(3), 233-240.
Manunta, G. (1999). What is security? *Security Journal, 12*(3), 57-66.
Manunta, G. (2002). Risk and security: Are they compatible concepts? *Security Journal, 15*(2), 43-55.
Markham, K. M., Mintzes, J. J., & Jones, M. G. (1994). The concept map as a research and evaluation tool: Further evidence of validity. *Journal of Research in Science Teaching, 31*(1), 91-101.
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.
McGill, W. L., Ayyub, B. M., & Kaminsky, M. (2007). Risk Analysis for Critical Asset Protection [Electronic resource]. *Risk Analysis, 27*(5), 1265-1281.
Morgan, G., & Henrion, M. (1990). *Uncertainty: a guide to dealing with uncertainty in quantitative risk and policy analysis*. New York: Cambridge University Press.
Norman, D. A. (1983). Some observations on mental models. In D. Gentner & A. L. Stevens (Eds.), *Mental models* (pp. 7-14). Hillsdale, NJ: Lawrence Erlbaum Associates Inc.
Novak, J.D., & Gowin, D. B. (1984). *Learning how to learn.* Cambridge: Cambridge University Press.
Novak, J. D. (1990). Concept mapping: A useful tool for science education. *Journal of Research in Science Education, 27*, 937-949.
Novak, J. D. (1998). *Learning, creating and using knowledge: Concept maps as facilitative tools in schools and corporations*. Mahwah: Lawrence Erlbaum Associates.
Pennebaker, J. W., Francis, M. E., & Booth, R. J. (2001). *Linguistic inquiry and word count (LIWC2001)*. Mahwah, NJ: Erlbaum Publishers.
Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.
Reisberg, D. (2001). *Cognition: Exploring the science of the mind* (2nd ed. ed.). New York: W. W. Norton & Company.
Rennie, L. J., & Gribble, J. (1999). *A guide to preparing your application for candidacy*. Perth, Western Australia: Curtin University of Technology.
Risk Management Institute of Australasia. (2007b). Security Risk Management Body of Knowledge. Retrieved 24 January 2007, 2007, from http://www.securityprofessionals.org.au/2007SRMBOK.htm
Ruiz-Primo, M. A., Schultz, S. E., Li, M., & Shavelson, R. J. (2001). Comparison of the reliability and validity of scores from two concept-mapping techniques. *Journal of Research in Science Teaching, 38*(2), 260-278.
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. (1984). *Learning astronomy and the organisation of astronomy concepts in semantic memory*: Unpublished doctoral thesis, Murdoch University, Perth, Western Australia.
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.
Smith, C. L. (2003). Understanding concepts in the defence in depth strategy. *Security Technology, 2003. Proceedings, IEEE 37th Annual 2003 International Carnaham Conference* pp. 8-16).
Standards Australia. (2004a). *AS/NZS4360:2004 Risk management*. Sydney: Standards Australia International Ltd.
Standards Australia. (2004b). *AS/NZS 4360: 2004 Risk Management* Standards Australia.
Standards Australia. (2004c). *HB221 Business continuity planning*. Sydney: Standards Australia International Ltd.
Standards Australia. (2004d). *HB436:2994 risk management guidelines: Companion to AS/NZS4360:2004*. Sydney: Standards Australia International Ltd.
Standards Australia. (2006). *HB 167:2006 Security risk management*. Sydney: Standards Australia.
Standards Australia. (2009). *AS/NZS ISO31000:2009 Risk management - Principles and guidelines*. Sydney: Standards Australia.
Stein, E. W. (1997). A look at expertise from a social perspective. In P. J. Feltovich, K. M. Ford & R. R. Hoffman (Eds.), *Expertise in context: Human and machine* (pp. 181-194). Menlo Park, CA: The MIT Press.
Streveler, R., Miller, R. L., & Boyd, T. M. (2001). Using an on-line tool to investigate chemical engineering seniors' concept of the design process. *Paper presented at the Annual Meeting of the American Educational Research Association, Seattle, WA.*
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.
Trochim, W. M. K. (1989b). An introduction to concept mapping for planning and evaluation. *Evaluation and Program Planning, 12*(1), 1-16.
Trochim, W. M. K. (1993). The reliability of concept mapping. Retrieved 24 July 2005, 1994, from http://www.socialreserachmethods.net/reserach/Reliable/reliable.htm
Trochim, W. M. K. (2005b). Concept mapping. Retrieved 28 July 2005, 2005, from http://www.socialresearchmethods.net/kb/conmap.htm
Trochim, W. M. K., & Cook, J. A. (1994). Using concept mapping to develop a conceptual framework of staff's views of a supported employment program for persons with severe mental illness. *Journal of Consulting and Clinical Psychology, 62*(4), 766-775.
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.
Wallace, A., Schirato, T., & Bright, P. (1999). *Beginning university: Thinking, researching and writing for success.* Sydney: Allen & Unwin.
Zedner, L. (2009). *Security: Keys ideas in criminology*. London: Routledge.