1-1-2011

Security risk management in the Asia Pacific region: what are security professional using?

David J. Brooks
Edith Cowan University

Hamish Cotton
Edith Cowan University

DOI: 10.4225/75/57a00f0dac5c1
4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

SECURITY RISK MANAGEMENT IN THE ASIA PACIFIC REGION: WHAT ARE SECURITY PROFESSIONAL USING?

David J. Brooks and Hamish Cotton
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
d.brooks@ecu.edu.au; h.cotton@ecu.edu.au

Abstract

The Asia Pacific (APAC) region encompasses a heterogeneous group of nation-states. Like the APAC region, the security industry operates within a diverse and multi-disciplined knowledge base, with risk management being a fundamental knowledge domain within security. Nevertheless, there has been limited understanding of what security professionals use when applying security risk management.

The study was designed to gain a better understanding of risk management practice in place throughout APAC. Questions were generated to gauge an understanding of current practice and levels of implementation of standards and frameworks. Participants were drawn from many industries, using non-probabilistic sampling methods in a "snowball" response to an online survey. Results were collected and analysed to provide interpretations and findings, and where appropriate, weighted factor analysis were conducted.

Findings indicated that the majority of APAC nation-states do not have a defined risk management standard, but security practitioners use their own internal framework. Following this approach, security practitioners use ISO 31000 and AS/NZS 4360 standards in parity, even considering their differing age. ISO 28000 Supply Chain Security Management was a popular standard, driven from Singapore. Nevertheless, the use of these standards should still raise concern due to a lack of a directed security risks management frameworks that incorporates threat, vulnerability and criticality. Further study needs to better understand what risk management techniques and frameworks security practitioners are using.

Key words

Risk management; security risk management; Asia Pacific; ISO 31000:2009; compliance

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) and this has begun to embed into the Asia Pacific (APAC) region (Cubbage & Brooks, In press). Risk management is now a well established discipline, with its own body of knowledge and domain practitioners. Nation-states worldwide have their own risk management standards and in many of these nation-states, it is the senior company executives who have responsibility to ensure that appropriate risk management practices meet internal and external compliance requirements (Brooks, 2011). 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 (Brooks, 2011).

Background and Significance of the study

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). 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) minimize potential harm, whilst capitalizing on potential opportunities (Garlick, 2007). 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, 2007; Cox, 2008; Manunta, 2002). It could be argued that a probabilistic approach does not provide efficacy for security, as security risk management has to take a greater heuristic approach.

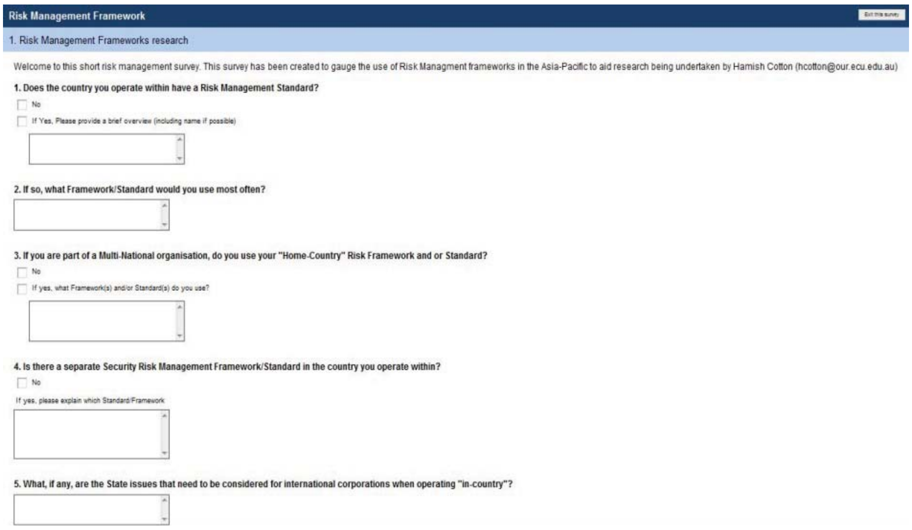
There are a number of nation-state international standards that consider risk management, but how used are these within the APAC practice area of security? Today, all parts of an organisation will use risk management to some degree and security is no different. Global standards such as ISO 31000:2009 is perhaps the benchmark. But the perceived view of this standard is currently being evaluated by a global survey (Dali, 2011), using many different risk groups. Furthermore, the security use of ISO 31000:2009 may be flawed, as it neglects to raise and integrate specific security risk concepts such as threat, vulnerability and criticality (Brooks, 2011), unlike AS/NZS HB 167:2006 Security Risk Management that incorporates these concepts into an integrated framework.

Study objectives

The study addressed a discrete Research Question, namely: *What risk management standard or framework do security practitioners use in the Asia Pacific region?* This overarching question allowed a number of discrete issues to be considered, such as the use of "in country" or "home country" security risk standards and frameworks? In addition, are there separate APAC "in country" security risk management standards and finally, do nation-states issues affect security risk management across the region?

STUDY DESIGN

The study conducted online surveys, which allowed for both quantitative and qualitative information gathering across the broad geographical area of the Asia Pacific (APAC). An initial number of APAC security practitioners were sourced, based on their known standing in the security management community. Each participant was asked to recommend additional leading risk management practitioners. From peer recommendations, additional practitioners were contacted until the study sampling size (N=35) was attained using a snowball effect. On contact, each practitioner was given access to the on-line survey tool (Figure 1). An on-line survey was administered to the practitioners due to the diverse geographical spread of the practitioners. All responses were anonymous, and information such as IP addresses and locations were not collected to enable the participant's to speak as freely as possible.



Risk Management Framework

1. Risk Management Frameworks research

Welcome to this short risk management survey. This survey has been created to gauge the use of Risk Managment frameworks in the Asia-Pacific to aid research being undertaken by Hamish Cotton (hcotton@our.ecu.edu.au)

1. Does the country you operate within have a Risk Management Standard?

□ No

□ If Yes, Please provide a brief overview (including name if possible)

2. If so, what Framework/Standard would you use most often?

3. If you are part of a Multi-National organisation, do you use your "Home-Country" Risk Framework and or Standard?

□ No

□ If yes, what Framework(s) and/or Standard(s) do you use?

4. Is there a separate Security Risk Management Framework/Standard in the country you operate within?

□ No

If yes, please explain which Standard/Framework

5. What, if any, are the State issues that need to be considered for international corporations when operating "in-country"?

Figure 1. On-line survey snap shot

The on-line survey contained the questions outlined below:

1. Does the country you operate within have a Risk Management Standard?
2. If so, what Framework/Standard would you use most often?
3. If you are part of a Multi-National organisation, do you use your "Home-Country" Risk Framework and or Standard?
4. Is there a separate Security Risk Management Framework/Standard in the country you operate within?

5. What, if any, are the nation-state issues that need to be considered for international corporations when operating "in-country"?

6. Please show which country you operate within in the text box below

After a set period, results were collected, processed and analysed to provide interpretations and findings. Due to the majority of respondents operating within the Australasia, where appropriate, weighted factor analysis was conducted. In addition, some of the respondents operated in multiple nation-state's, so responses that indicated consistent practice have been added to represent each state.

ANALYSIS

The collected data was analysis, presented in the sequence of the posed survey question.

Q1: Does the country you operate in have a Risk Management Standard?

The result of the survey Question 1 indicated that many of the Asia Pacific nation-states do not have a risk standard (Figure 2).

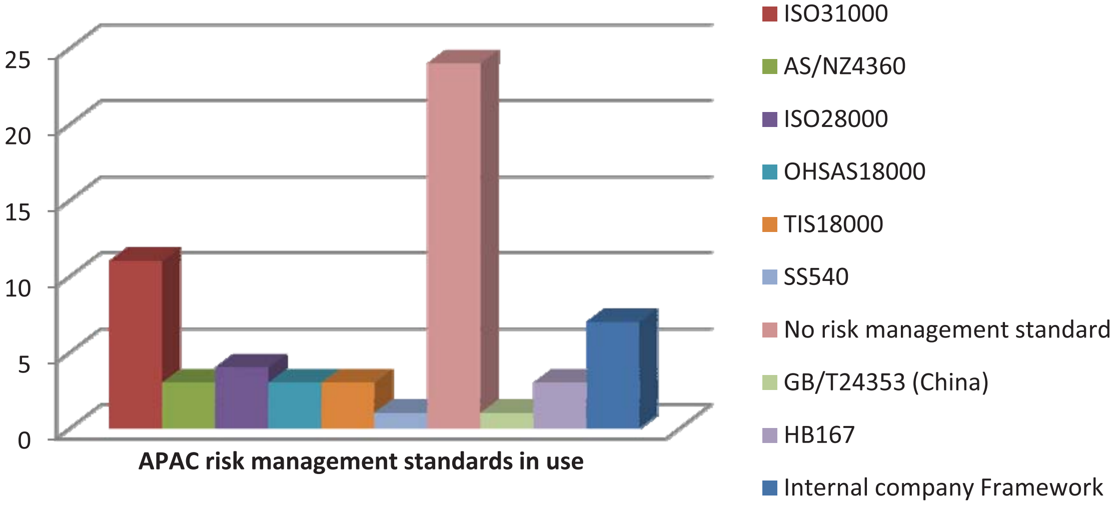


Figure 2. APAC risk management standards

When the same participant responses were weighted, to allow for a cross sample representation of nation-states, the results indicated no significant change. A significant number of the respondents indicated that the in-country nation-states did not have a risk management standard (Figure 3). Both ISO 31000 and AS/NZS 4360 are reflected as the two most popular responses after “no risk management standard”; however, there is a levelling over the remaining frameworks that indicates that although ISO 31000 is often the “in-country” risk framework, many other frameworks are in place among the various APAC nation-states.

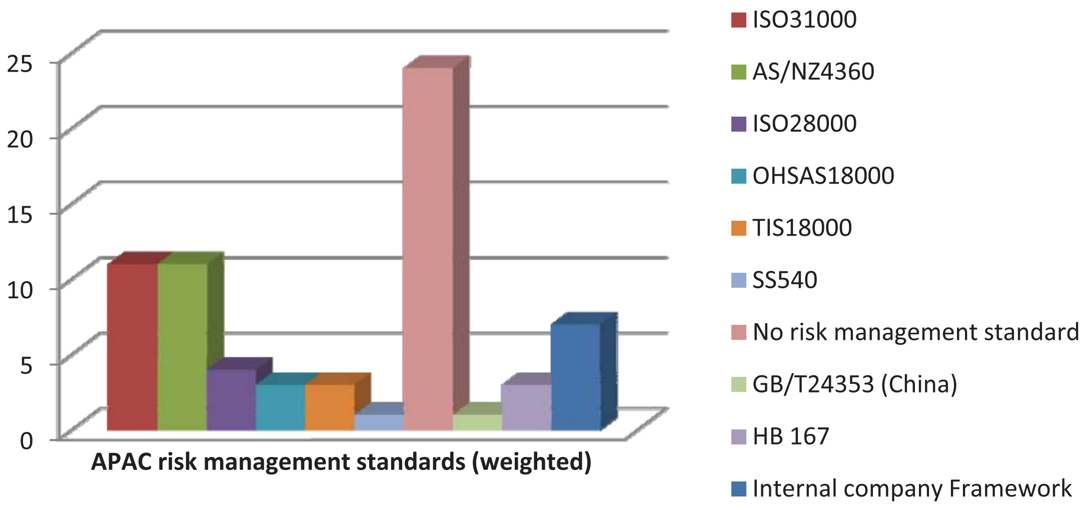


Figure 3. APAC risk management standards (weighted)

Q2: What Framework or Standard would you use most?

Question 2 represented the most used frameworks, whether it is an in-country standard as mentioned in Question 1 or any other standard. As illustrated, the "no risk management standard" remains the most popular approach (Figure 4). Of the companies surveyed, the most used framework was ISO 31000 with internal risk management standards proving to be the next most popular approach.

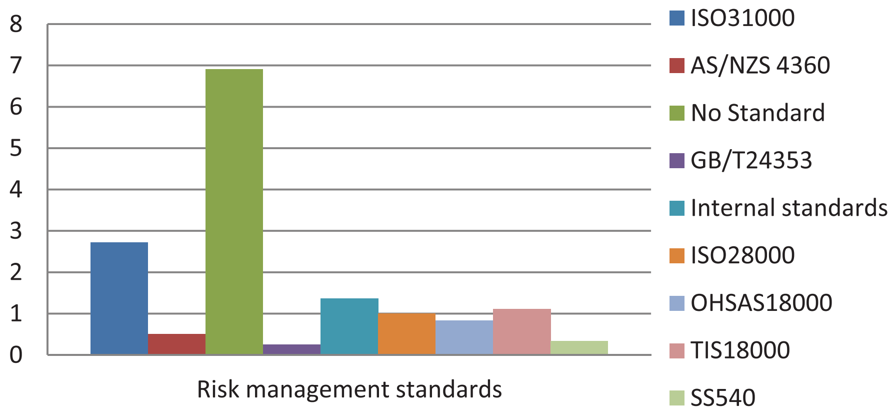


Figure 4. What framework would you use?

When Question 2 results were weighted to represent each nation-state equally, the results indicate a large number of risk professionals are using AS/NZS 4360 and "Internal" standards in an almost equal measure (Figure 5). In addition, the amount to which the companies within each nation-state use no risk management standard or ISO31000 reduces significantly. One of the standards that come to the fore shows the more widespread use of ISO 28000, which is primarily focussed toward supply chain management. An interesting result is the parity of the older AS/NZS 4360:2004 and the newer ISO 31000:2009.

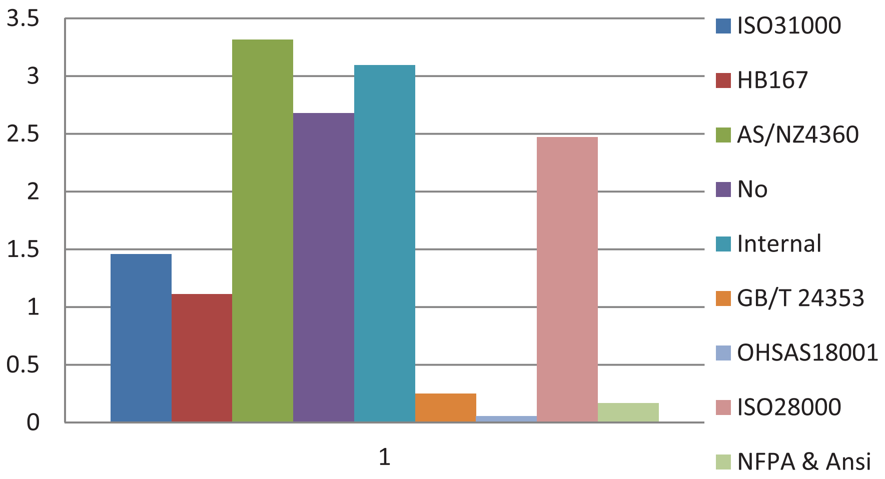


Figure 5. What framework would you use (equal weighting)

Q3: As an International company, do you use your "Home-Country" framework?

Question 3 gauged the application of "home country" risk management frameworks within the international corporate environment. The results indicated (Figure 6) that two-thirds of the respondents did not use their home country risk management standards. Although this survey did not seek to understand "why", a number of factors may influence this response including legislative requirements, compliance and the overall lack of implementation of risk management frameworks and standards among those surveyed.

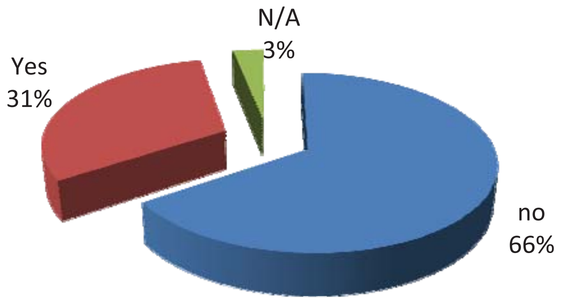


Figure 6. International companies use of "Home-Country" risk frameworks

Q4: Is there a Security Risk Management framework in-country?

Question 4 attempted to understand whether separate risk management frameworks existed with in-country operations. The participants indicated in the affirmative (78%), that there were no local security risk management standards (Figure 7). Whether frameworks exist, or whether the practitioners were unaware of them. This can be demonstrated by the 5 participants (n=8) answering "no" from Australia.

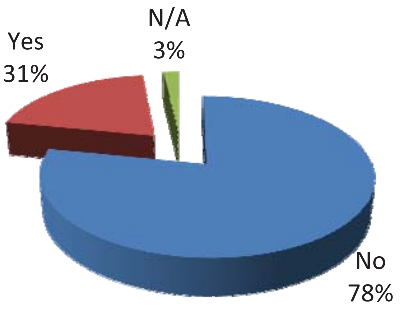


Figure 7. Separate security risk management framework in-country operation?

Q5: Issues for international corporations when operating "in-country"?

This question represents the qualitative aspect to the survey, by attempting to understand the barriers of working within foreign environments. The resulting comments (Table 1) ranged greatly, from no significant barriers through to issues of corruption and compliance. Of interest is the focus of many of the respondents on compliance and legislative issues. These issues appear to be at odds with survey Questions 1 to 3, which indicated that many companies in a number of nation-states do not implement a risk management standard. In addition, that a large proportion used “no framework”, the older AS/NZS 4360 standards or internal risk management systems.

Table 1. What are the in-country nation-state risk management issues?

Participant written responses (simplified)
Abide by the law.
Ensuring compliance with State Laws, including Industrial laws.
Legal obligations. Good Corporate Citizenship and obtaining "buy in" from local employees.
Corruption, ISPS and processes for obtaining assigned Government security support.
Remain vigilant, as people will attempt to defraud you from within and extort you from outside.
Host country issues most relevant to the multi-national I work for are commercial (tax, residency, legal etc).
A very open ended question. XXXX[1] being a diverse and vibrant country attracts a great deal of foreign investment, entities operating within confronted with diverse and vibrant threats and risks.
Legislative changes.
Political, IR/HR issues, workplace safety, regulatory/compliance matters
There should be local legislations that are compulsory for companies to follow.
Regulatory requirements.
Legislative requirements that require compliance within an in-country set of standards and may differ from global internal company standards.
Need to be globally consistent, but regionally flexible.
(1) The English common law "duty of care" principle; (2) legal aspects pertaining to negligence; (3) occupational health and safety laws; & local fire safety codes.
Business Continuity Management issues.
Local regulatory requirements pertaining to business and corporate governance.
Legal frameworks, HSE, cultural issues, risk acceptance
Local procurement process, including the need to have a local company as a representative.

Note 1: XXXX = Nation-state removed to maintain ethics anonymity

FINDINGS AND RECOMMENDATIONS

The survey represented a number of nation-states and their practitioners within the Asia Pacific region. Findings allowed a response to the posed Research Question, being *What risk management standard or framework do security practitioners use in the Asia Pacific region?* In responding to the research question, a list of used frameworks or standards are listed and described. In addition, the limited or extensive use of these frameworks, the issue of governance and the unique nature of security risk management are considered.

The many approaches to Risk Management

There are a number of risk management and security risk management frameworks used by the security industry (Table 2) in APAC.

Table 2. Risk Management Standard or Framework

Standard or Framework	
ISO 31000: 2009 Risk Management	Singapore Standard SS540 (BCM)
AS/NZS Handbook 167:2006 Security Risk Management	ISO 28000 Supply Chain Security Management
NFPA 1250: Practice in Emergency Service Organization Risk Management	TIS 18000 Guide to OH&S Management Systems
RMIA SRMBOK	AS/NZS 4360:2004 Risk Management

AS4360 Risk Management (now obsolete)

AS/NZS 4360:2004 Risk Management (Standards Australia, 2004) 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). The standard was widely used by security professionals within Australia and became the draft for the International Standards Organisation ISO 31000:2009 Risk Management (Standards Australia, 2009, p. vi). The standard has now been replaced by AS/NZS ISO 31000:2009.

ISO 31000:2009 Risk Management

ISO 31000:2009 Risk Management presents a framework (Figure 8) or process (Standards Australia, 2009, p. vi) for risk management. What the 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 AS/NZS HB167:2006 Security Risk Management.

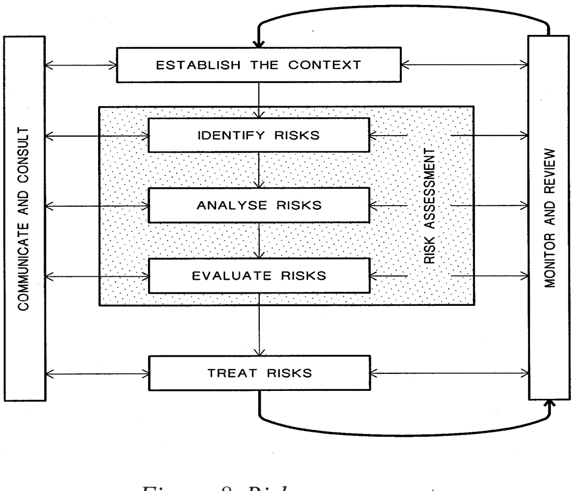


Figure 8. Risk management.

(Standards Australia, 2004)

Singapore Standard SS540 (BCM)

Singapore Standard SS540 is a framework for organization to analyse, implement strategies, process and procedures in continuity. The standard focuses on resilience and protection of critical assets, human, environment, intangible and physical, taking a continuity management and recovery of critical business functions approach. The standard aims to provide policy, procedures and process to prevent, prepare, respond and recover (Heng, 2008).

AS/NZS 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" (2004, p. 2). The handbook "provides 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 9); all significance and unique to this domain of risk management (Brooks, 2011).

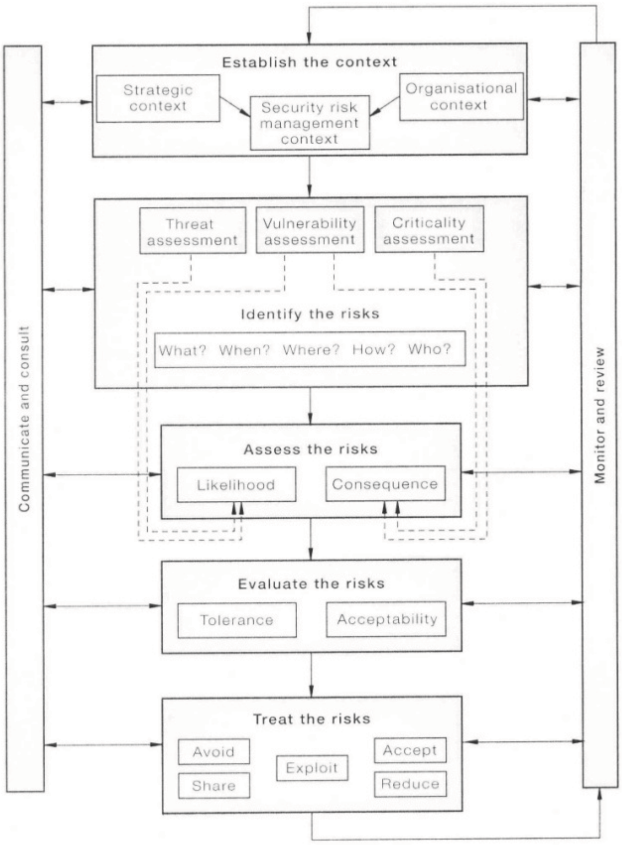


Figure 9. HB167:2006 Security risk management framework.

(Standards Australia, 2006, p. 14)

NFPA 1250: Practice in Emergency Service Organization Risk Management

Practice establishes minimum criteria to develop, implement or evaluate an emergency service organization risk management program for effective risk identification, control and financing of fire departments and organisations. The standard incorporates all frameworks that a fire authority could implement and use as a model to ensure compliance within the wider jurisdiction of risk management and contingency planning.

ISO 28000 Supply Chain Security Management

ISO 28000 standard attempts to reduce risks to people and cargo within the supply chain. The standard address potential security issues at all stages of the supply process, thus targeting threats such as terrorism, fraud and piracy. ISO 28000 specifies the requirements for a security management system to ensure safety in the supply chain. This standard appears to be driven strongly from the Singapore government.

TIS18000 Guide to Occupational Health and Safety Management Systems

Thailand's TIS18000 has been established based on the British Standard, BS 8800:1996 Guide to Occupational Health and Safety Management Systems. Currently, there are two series of standard being: TIS 18001: Occupational Health and Safety Management System: Specification, and (2) TIS 18004: Occupational Health and Safety Management System: Technical Guides on Implementation of OSH-MS.

Security Risk Management Body of Knowledge (SRMBOK)

An Australian Federal Government supported initiative with RMIA resulted in the SRMBOK framework and guide for practitioners (Talbot & Jakeman, 2008). 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, 2007, p. 1).

Limited use of frameworks

Perhaps the most interesting finding is that no specific frameworks or standards are implemented by many working practitioners within the security risk management field. Such an issue can be caused by the diverse issue of limited professionalism in the industry. To be professional requires enforced standards of behaviour/ethics, standards of education, formal requirement for professional development, a college of peers and a distinct body of knowledge (The Interim Security Professionals Taskforce, 2008, p. 10). A distinct body of knowledge for corporate security includes security risk management (Brooks, 2011), a view supported by other such as Risk Management Institute of Australasia (RMIA) (Talbot & Jakeman, 2008) and ASIS International (2009). Analysis could argue that professionalism is lacking, as the use of theoretical security risk management frameworks would be what is expected of professional practitioners.

Use of ISO 31000

The study found that ISO 31000 was used, but this was relatively restricted and far less than the Australian Standard AS/NZS 4360. In the past, the predecessor of ISO 31000:2009 was AS/NZS 4360. This standard was often considered "almost a de facto global standard" (Jay, 2005, p. 2) and has become an international template on dealing with risk. It has been used extensively by security and risk professionals across Australia (Beard & Brooks, 2006, p. 5; Jones & Smith, 2005, p. 2) and Asia Pacific. Nevertheless, it could be argued that ISO 31000 should provide risk management and security risk management with its underlying framework due to its international status.

Significant use of AS/NZS 4360

Of the responses citing adherence to risk management frameworks, a significant number of respondents indicated adherence to the now superseded AS/NZS 4360:2004 Standard. Many of the participants highlighted the need for ongoing training and education in the risk management profession towards a more holistic framework, incorporating an element of resilience as demonstrated with ISO 31000. Nevertheless, resilience is still developing and expanding; with early embodiments of Organisational Resilience originating in the United Kingdom from Continuity Management and the United States from Security Management (Brae & Brooks, 2011). Another explanation could be that the risk framework set out by AS/NZS 4360 is seen as an adequate response to risk in a corporate environment, with issues of resilience falling to other areas of the corporate model.

Corporate Governance

Issues of corruption and legal compliance are reflected quite broadly across all responses. This issue raises the question; is this unique to the Asia Pacific region? Or a broader problem within the security risk management field. Compliance issues were also prominent; however, this is also reflected in some of the standards and frameworks mentioned throughout the study. As the Thai Industrial standards reflected, a number of standards are heavily based on ISO 31000 with individual nations-states issuing new standards which allow for certification.

Unique nature of SRM

The study clearly indicated a lack of formal or informal security risk management frameworks or standards. As Standards Australia suggested, “the field of security risk management is rapidly evolving” (2004, p. 2). Security risk management is a unique sub-domain of risk management (Brooks, 2011) demonstrated through a number of concepts such as threat, criticality and vulnerability. *Threat* is a critical factor when considering security risk; however, ISO 31000:2009 does not present this concept or other security related concepts like *vulnerability*. It could be argued that with use of such standards as ISO 31000 and AS/NZS4360, that security practitioners lack this specific sub-domain knowledge to ensure efficacy in security risk management.

METHODOLOGICAL IMPLICATIONS

Methodological limitations of the study were identified and included the need for a greater and broader sample. For greater statistical confidence, the sample 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 study’s findings; nevertheless, conclusions made have to be considered within the context of the study.

FURTHER RESEARCH

The study has led to the need for greater research in certain aspects of security risk management. These issues include an extended understanding of what standards, frameworks or process practitioners are doing when and if they use security risk management. Why is an obsolete standard still used extensively and why is ISO 31000 not making greater propagation into the Asia Pacific region? Some of these issues may be addressed with the current global survey of ISO 31000 underway (Dali, 2011); however, beyond this survey is the need for a greater security driven risk management understanding.

CONCLUSION

Risk management and to some degree, security risk management, have flourished over the past decade and are relied upon to provide robust and informed mitigation strategies in the protection of 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. In addition, within the broad heterogeneous region of Asia Pacific, what frameworks or standards are security practitioners using?

The study used a non-probabilistic on-line survey of security practitioners in the Asia Pacific region, in an attempt to gauge what security risk management frameworks security professionals are using. The study found that a broad range of standards were being used, such as ISO 31000, ISO 28000, Singapore Standard SS540 and Australian Standard AS/NZS 4360, to name a few. These many standards were described, providing a brief synthesis of each. Nevertheless, the most used framework was the “internal framework”, although the extent and approach of this framework certainly requires more in-depth research. Furthermore, many of the Asia Pacific nation-states have no risk management or security risk management standard.

An issue that requires greater discussion is the lack of security risk management standards. Generic risk management lacks core security risk management concepts, such as threat, criticality and vulnerability. Therefore, there is a greater need for directed security risk management standards, preferable at the international level using an ISO standard. Further research needs to use a larger and more diverse sample, to better understand what “internal frameworks” are being used and the make-up of these frameworks.

REFERENCES

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

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

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.

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.

Brae, B., & Brooks, D. J. (2011). *Organisational Resilience: Understanding and identifying the essential concepts.* Paper presented at the SAFE 11: 4th International Conference on Safety and Security Engineering, Antwerp, Belgium.

Brooks, D. J. (2011). Security risk management: A psychometric map of expert knowledge structure. *International Journal of Risk Management, 13*(1/2), 17–41. doi: 10.1057/rm.2010.7

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.

Cubbage, C., & Brooks, D. J. (In press). *Corporate security in the Asia Pacific region: Crisis, crime, fraud and misconduct*. New York: Francis & Talyor.

Dali, A. (2011). Global survey on ISO 31000 risk management standard Retrieved October, 18, 2011, from http://www.linkedin.com/groups?mostPopular=&gid=1834592

Garlick, A. (2007). *Estimating risk: a management approach*. Aldershot: Gower Publishing Company.

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

Jones, D. E. L., & Smith, C. L. (2005). *The development of a model for testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS 4360:2004 - Risk Management*. Paper presented at the Recent advances in counter-terrorism technology and infrastructure protection, Proceedings of the 2005 Science, Engineering and Technology Summit 2005 Canberra, Australia.

Manunta, G. (2002). Risk and security: Are they compatible concepts? *Security Journal, 15*(2), 43-55.

Morgan, G., & Henrion, M. (1990). *Uncertainty: a guide to dealing with uncertainty in quantitative risk and policy analysis*. New York: Cambridge University Press.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

Risk Management Institute of Australasia. (2007). Security Risk Management Body of Knowledge. Retrieved 24 January, 2007, from http://www.securityprofessionals.org.au/2007SRMBOK.htm

Standards Australia. (2004). *AS/NZS4360:2004 Risk management*. Sydney: Standards Australia International Ltd.

Standards Australia. (2006). *HB 167:2006 Security risk management*. Sydney: Standards Australia International Ltd.

Standards Australia. (2009). *AS/NZS ISO31000:2009 Risk management - Principles and guidelines*. Sydney: Standards Australia International Ltd.

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

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