SECURITY RISK MANAGEMENT: A DANGEROUSLY OVERRATED AND BROKEN PARADIGM

Anshin Consulting

Identifying those persons with an intent to harm you

ABN: 64 606 695 809

ACT Master licence: 17502351

NSW Master licence: 000102816

SECURITY RISK MANAGEMENT: A DANGEROUSLY OVERRATED AND BROKEN PARADIGM

Author: David Harding

              Anshin Consulting

              30 January 2016

Abstract

As humans we use a variety of systems to structure our beliefs and behaviours to better understand the world in which we live. We call these concepts cultures, paradigms and worldviews, and adapt different cognitive and linguistic competencies to better understand and explain them. For almost two decades, both government and private protective security cultures have focused on the premise that Risk Management and Security Risk Management provide a construct and conceptual base to reduce the likelihood of criminal attack. This conceptual base, or paradigm, has been developed, and in some cases legislatively enforced, to provide protection from harm for individuals and organisations. It is strongly believed within the protective security services, government and private enterprises that by applying Risk Management, and specifically Security Risk Management principles to intentional criminality issues, it will be possible to reduce the likelihood of harm and criminal incidence.

This paper will provide a background to the current paradigm, and identify the importance of the paradigm within the protective security field. This paper will also, through statistical analysis of criminal incidence, identify that general criminal incidence has been decreasing

within Australia for almost two decades. However, in areas where Risk Management and Security Risk Management practices have been implemented, the incidence of criminality has increased. Although difficult to identify the specific causal nature of this trend of criminal incidence, these opposing trends suggest and are indicative of a structural issue within the Risk, and Security Risk Management paradigms.

SECURITY RISK MANAGEMENT: A DANGEROUSLY OVERRATED AND BROKEN PARADIGM

Every era has its own set of concepts of self, cultures and worldviews. Within each culture there is also a variety of paradigms that provide the best way to explain our relationship to the world around us. This not only applies to the era and times that we as a culture and society live in, but also at an individual level as well. As humans we use these systems to structure our beliefs and behaviours in a way to better understand and explain the world we live in. To adapt to these varying structures, the individual applies cognitive and linguistic competencies to better understand and then explain different concepts.

For almost two decades both government and private protective security cultures, that is those beliefs and behaviours inherent within the industry, have focused on the belief that Risk Management and Security Risk Management provide a construct and conceptual base that can reduce the likelihood of criminal attack. This conceptual base, or paradigm, has been developed, and in some cases legislatively implemented so as to provide protection from harm for individuals and organisations. It is strongly believed within the protective security services, government and private enterprises that by applying Risk Management, and specifically Security Risk Management principles to intentional criminality issues, it will be possible to reduce the likelihood of harm and criminal incidence.

This paper will provide a background to the current paradigm, and identify the importance of the paradigm to the protective security field. This paper will also, through statistical analysis of criminal incidence, identify that within Australia the general rate of criminal incidence has been decreasing for almost two decades. However, in some areas where Risk Management and Security Risk Management practices have been implemented, the incidence of criminality has increased. This counter trend of criminal incidence is indicative of a structural issue within the Risk, and Security Risk Management paradigm.

1. BACKGROUND

The social contract that is said to exist between the State and individual involves the protection of the individual by the State, and in return the individual accepts the forfeiture of certain freedoms. To ensure the internal safety and security of the State's individuals, the State provides a variety of services and conditions to protect the State's varying communities from harm. This also applies to the State providing protection to its own staff and organisations.

In Australia, this contract means that "the first role of government is the nation's security" (Rudd 2008). In application within Australia, which this paper will focus on, the Australian government, and the varying state and territories provide a variety of Environmental, Developmental and Situational measures that are aimed at reducing or preventing harm through criminal acts to its citizens (Morgan, Boxall, Lindeman, & Anderson 2011, p. 12). Specifically, the Environmental approach seeks to change the specific environment that may cause criminal events to occur and contains broad planning initiatives and situational approaches (Morgan et al. 2011, p. 13). Situational Crime Prevention, is achieved through changing the situation that an offender may find themselves in, by removing or reducing the opportunities that the offender has to commit their desired offence (Morgan et al. 2011, p. 13). Some examples include the use of methods to increase the effort to commit a crime, such as target hardening or controlling the access to facilities (Cornish & Clarkes 2003, p. 90). Another approach called Crime Prevention Through Environmental Design (CPTED) and urban renewal projects, seek to reduce the opportunities for criminal events through design and management of building and landscaped environments (Morgan et al. 2011, p. 14). Examples of CPTED can include the provision of natural surveillance opportunities, well-lit pedestrian thoroughfares or fewer places for potential offenders to hide (Morgan et al. 2011, p. 14).

In addition, government can also focus on Social Crime Prevention initiatives that seek to prevent crime through influencing the underlying social and economic causes that motivate an offender to commit a crime (Morgan et al. 2011, p. 15). Examples can include the provision of housing, education, health and community cohesion initiatives (Morgan et al. 2011, p. 15).

In Australia, many businesses also accept some responsibility for the protection of their assets and employees. This occurs though the application of measures that are designed to remove or reduce the opportunity that a potential offender has to commit a harmful action against the business (Queensland Government 2015). In addition, government and many businesses seek to reduce the likelihood of harmful attacks and the consequences that the attacks may cause through the application of measures and processes that manage these risks. This concept and the framework that comes from it, is called Risk Management (International Organisation of Standardization 2009, p. iv).

Since the early 1990's the concept of Risk Management has emerged as a well established discipline with its own body of knowledge. This concept has been adopted widely by both government and private sectors (Brooks 2011, p.1). More recently, processes designed to reduce the likelihood of deliberate harmful attacks by criminal offenders has been incorporated into the concept and documented in the Standards Australian Hand Book HB: 167:2006 and termed Security Risk Management (Standards Australia 2006, p. 11). Indeed, in some jurisdictions within Australia, the use of the concept and process knowledge of Risk Management has been legislated and enforced (Parliament of New South Wales 1997, Part 2 Division 3 Section 21A).

But does the implementation of Security and Risk Management processes prevent or reduce the likelihood of attacks by criminal offenders?

Does the specifically developed processes outlined in the Standards Australian Hand Book HB 167:2006, warrant the seemingly importance provided to it?

2. THE PARADIGM BUBBLE

Although the term 'security' itself means free from danger (Merriam-Webster Dictionary), the term has undergone significant change brought on by the interrelationships within the international system. Here, interpretations can vary between rationalist approaches to the threat of military challenges to sovereign states, to the neo-liberalist view of challenges that may threaten society's security (Goetschel 2000). The leading international security association ASIS International defines security to be "the condition of being protected against hazards, threat, risks or loss" (ASIS 2012, p. 59). The previously mentioned Standards Australian Handbook HB 167:2006 defines security to be "the preparedness, protection and preservation of people, property and information both tangible and intangible" (Standards Australia 2006, p. 11). Finally, numerous states within Australia define the term by providing an outline to the types of employment that may be undertaken. For instance, in the New South Wales Security Industry Act of 1997, the legislation does not define the term, but provides an outline as to the types of activities that persons who are employed within that industry can undertake. These activities may include the roles of security guarding, body guarding, control room monitoring, the providing of advice or equipment designed to minimise the security risk to an individual or organisation, or enhance the protection of any property (Parliament of New South Wales 1997, Part 1 Section 4). Given these varying definitions, this paper will adopt a broad view of the definition, and take security to be the protective means to provide protection from threat and risk of harm.

In a similar fashion, the concept of Security Risk Management can have varying definitions. The Hand Book developed by Standards Australia HB 167:2006, defines Security Risk Management as "the culture, processes and structures that are directed towards maximising benefits and minimising disbenefits in security, consistent with achieving business objectives" (Standards Australia 2006, p. 11). Alternatively, The Australian Auditor General sees Security Risk Management as the management of an "event that could result in the compromise of official resources, including personnel, measured in terms of its likelihood and consequences" (Auditor-General 2008, p. 7). Meanwhile, the Australian Attorney General's Department's, Protective Security Policy Framework (PSPF) identifies Security Risk Management as processes to identify specific risks to an agencies people, information and assets, and the management of appropriate protections to remove or reduce those risks (Attorney-General's Department 2010, p. 12). Again, considering these varying definitions, this paper will define Security Risk Management as the processes taken to reduce the risk of an incident, actioned by an individual or group with intention to cause a negative consequence.

2.1.1 The Importance of Risk Management and Security Risk Management

The importance of Security Risk Management within the Australian security context cannot be understated. For instance, the Attorney General's Department within the Australian Government is responsible for the development and refinement of protective security policy, and does so through the Protective Security Policy Framework (PSPF) document. A

specific requirement of this policy document is that Agencies are required to develop Security Risk Management processes. The processes that must be followed are outlined in International Organisation of Standardisation (ISO) standard ISO 31000: 2009 Risk Management - Principles and Guidelines, and the Australian and New Zealand Standards Hand Book, HB 167:2006 Security Risk Management (Attorney-General's Department 2010, p. 13).

In addition, individual states have outlined through their individual mechanisms that those persons that provide specific advice and consultations as to protective requirements of organisations and individuals, must have appropriate levels of knowledge. For example, in NSW the Security Industry Act 1997 legislates that a person that acts as a Consultant that identifies and analyses security risks and provides solutions and management strategies must have a police commissioner approved licence (Parliament of New South Wales 1997, Part 2 Division 2 Section 12). Applicants for this licence must have as a minimum, a Certificate IV in Security and Risk Management with additional experiential requirements (NSW Police Force n.d.). In a similar vein, the Australian Capital Territory has requirements for advisory licensing (Office of Regulatory Services 2012, p. 10)

Based on the above examples of government policy and legislation, it is reasonable to believe that the acquisition of knowledge pertaining to security risk management is a prerequisite to the ability to determine ways, means and methods to reduce the likelihood and consequences of intentional criminal attacks both within government and private industry. The Security Risk Management Handbook HB 167:2006, states that Security Risk Management is a new paradigm, "which provides a means of better understanding the nature of security threats and their interaction at an individual, organisational, or community level" (Standards Australia 2006, p. 6). Indeed the Handbook further states that Security Risk Management "has become a powerful tool in assisting prevention and management of the consequences of events that are often outside an 'organisation's' normal understanding and experience" (Standards Australia 2006 p 10). As HB 167: 2006 notes, Security Risk Management introduces a new element into an organisations established risk management framework, that of a person intentionally introducing an exposure to harm by deliberately seeking to overcome controls that are in place (Standards Australia 2006, p. 11).This would mean that the proper application of the principles and methods outlined in the HB 167:2006 would assist an individual, organisation or community in the prevention of crime.

2.1.2 The Evidence

The Australian Institute of Criminology (AIC) compiles information from a broad range of sources to create a number of reports regarding crime and criminal justice in Australia (Australian Institute of Criminology 2014, p. iii). According to the AIC's recent report on the general trends of crime within Australia, published in 2014 and collating crime up to 2013, there has indeed been an overall reduction in crime rates across a variety of crime types (AIC 2014, p. iii). For instance, the rate of robbery crime, defined as "the unlawful taking of

property, without consent, accompanied by force or threat of force" (AIC 2014, p.25) has been generally falling since 2002 (AIC 2014, p. 3).

According to the NSW Justice Fact Sheet, these reductions in robbery incidences are made possible by the implementation of appropriate control mechanisms such as quality locks on doors, appropriate lighting and irregular banking procedures (Crime Prevention NSW). Although difficult to specifically assess, some may infer that the implementation of Security Risk Management's risk treatments, such as access control and security awareness programs, may have had some positive effects on general security awareness (Crime Prevention NSW). The implied result of these measures is that the utilisation of such measures as a risk treatment may result in effective crime prevention strategies.

3. BURSTING THE BUBBLE

However, taking credit for the previously mentioned drop in general crime rates since the implementation of Risk Management frameworks, which became legislated in some jurisdictions in 1999 with the implementation of AS/NZS 4360:1999, may be presumptuous. While general trends may have seen a decreasing of victimisation since the late 1990's, analysis of specific subpopulations that have had substantial inputs from the Risk Management and specifically the paradigm suggested from the Security Risk Management Handbook, show a different view.

The AIC has identified that the rate of robbery crime gradually rose during the late 1990's. Since that period, there has been a general downward trend in the rate of victimisation since 2001 (AIC 2014, p. 6). In addition, the AIC through the National Armed Robbery Monitoring Program, monitors and identifies trends in armed robbery across Australia (Smith, & Louis 2010a, p. 1). In the most recent publicly available information, the AIC identifies specific trends in armed robbery of among others, Cash in Transit (CIT) operations, pubs and licensed premises, retail, service stations and banking institutions (Borzycki, & Fuller 2014, p. 15).

It could be assumed that these commercial organisations would have through legislated corporate and insurance necessities, conducted security risk assessments and developed management plans to reduce the likelihood of criminal attack. If this is the case, and assuming appropriate assessments were conducted, it is likely that the rate of criminal attacks against these organisations should have decreased since the legislated implementation of Security Risk Management practices in the early 2000's, and specifically since 2006. However, this is not the case, and indeed it is the reverse trend that is evident.

3.1.1 Armed Robberies At Licensed Premises

The AIC identifies such premises as secure businesses due to the perceived level and complexity of the visible and assumed security measures that the premises utilises (Fuller 2014, p. 5). Such premises utilise situational crime preventative measures, or security treatment options such as strict cash handling procedures, additional onsite security, controlled access to different areas, and closed circuit television (Standards Australia 2006, p. 122). It could be assumed that with the implementation of these Security Risk Management security control mechanisms, the incidence of criminal attacks such as robbery would be reduced. In fact, the National Armed Robbery Report program has noted that between the years of 2004 and 2010, there was an increase of the incidents of armed robbery on these premises by 20% (Borzycki, & Fuller 2014, p. 4).

3.1.2 Service Stations

Service stations have increasingly been the target of armed robbery since the late 1980's (Smith, Louis & Preston 2009, p. 1). Service stations have introduced many security control measures which have included target hardening measures such as anti-robbery screens, surveillance systems, additional staff during night periods, and a variety of alarms and additional security guards (Cornish & Clarke 2003, p. 90, Smith, Louis & Preston 2009, p. 4). Again, it could be reasonable to assume that with these Security Risk Management security controls in place, the rate of criminal victimisation would decrease. However, between 2004 to 2006 there was a continued increase in the incident of criminal robbery of 31%, a trend which continues today (Borzycki, & Fuller 2014, p. 5, Smith, Louis & Preston 2009, p. 1).

3.1.3 Cast In Transit Operations

The Cash in Transit (CIT) industry involves the transportation, delivery and receipt of valuables such as cash, jewels, bullion and other financial instruments by road (Comcare 2009). This industry, which has undergone several Justice Commission inquiries, such as the Industrial Relations Commission of New South Wales in 1997 (Industrial Relations Commission of New South Wales 1997), which recommended that appropriate risk assessments should be conducted on all CIT delivery sites (Industrial Relations Commission of New South Wales 1997, p. 338). The industry routinely uses security controls such as uniformed and covert security guards, CCTV, armoured vehicles, specific counter-ambush procedures and secure storage of assets (Standards Australia 2006, p. 122).

Given this level of inquiry and implemented security control measures, it would be reasonable to expect that the industry takes reasonable precautions to reduce the risk of harm to its employees, especially those involved in the hazards of CIT operations. Interestingly though, between the years 1997 to 2000 there had been a drop in the incidence of robbery against CIT operations in Australia from pre 1997 levels (Smith & Louis 2010b, p. 3). However, since 2000 there has been an increase in attacks against CIT operations. This increase spiked between 2006 and 2008. Since that period, although there has been a slight decrease in attacks, the incident level continues to remain above five times pre 2000 rates (Smith & Louis 2010b, p. 3)

There is limited publicly available information and evidence, and only generalised case study and occurrence statistics that can be utilised to determine the reasons for these findings. However, it would appear at first analysis that if the organisations concerned followed the enforced methodology of HB 167:2006 and ISO 31000:2009 or its predecessors AS/NZS 4360:1999 and AS/NZS 4360: 2004, there should have been an increase in efficiency and effectiveness in the implemented preventative risk treatments. This should then produce a decrease at least matching the overall societal decrease, if not greater, in criminal attacks over a period of several years. This has not been the case.

Statistical analysis would indicate that should a large population data set indicate a general downward trend in incidents of criminal victimisation, it would be reasonable to expect that unless affected by specific outlying factors, a sub population of the original sample would also exhibit a similar general downward trend (Isotalo n.d, p. 51). As identified above, with regard to the general incidence of crime within Australia there has been a general downward trend in crime rates since the late 1990's. This has also been the case with smaller subset populations, such as the incidents of armed robbery during that period. It would be reasonable to expect that smaller population subsets, such as those identified as armed robbery of licensed premises, Cash in Transit operations and service stations would also follow this general trend. However, as identified above in the areas where there is an increase in security focus, and in some cases the legislated requirement to implement security control measures designed to reduce or remove the likelihood of crime, the incidence of crime has increased. Such an opposite trend in subordinate population data is significant and worthy of further examination to identify causal determinants.

Although given the limited data available it would be difficult to determine the causal nature of this significant trend. Indeed many other factors may be involved that are not being taken into account. However, ISO 31000:2009 Risk Management and HB 167:2006 Security Risk Management have been specifically developed and implemented to be a powerful tool in the prevention and management of the consequence of events outside of an organisations normal understanding (Standards Australia 2006, p. 10). Therefore, the identified opposing trend of general population data in comparison to the subordinate population data is indicative of a possible structural issue in the development of security practice methodologies.

4. CONCLUSION

This paper has sought to burst the paradigm bubble that Risk Management, and specifically Security Risk Management, is an effective way to treat the risk of criminal attack. This paradigm has been reinforced by government and industry bodies through legislative, industry practice and body of knowledge mechanisms.

This paper has identified that the overall incidence of criminality within Australian society has been generally decreasing since the late 1990's. However, as identified above, where the principles and methods of Risk Management and Security Risk Management have been implemented, the incidence of crime has tended to increase. This trend strongly suggests that the current utilisation of the principles and methods of security and risk management is counter-productive to the aim of reducing the risk of criminal attack. It also suggests that more detailed research and investigation should be conducted to determine why this situation has occurred, and possibly identify alternative methodologies that may reduce the risk of criminal attack. At present the paradigm is broken.

ACKNOWLEDGMENTS

REFERENCE LIST

ASIS International 2012, *Security Management Standard: Physical Asset Protection, ANSI/ASIS PAP.1- 2012*, American National Standard.

Attorney-General's Department 2010, *Protective Security Policy Framework, Securing Government Business*, Australian Attorney-General's Department, Canberra, viewed 20 January 2016, https://www.protectivesecurity.gov.au/Pages/default.aspx

Auditor-General 2008, *Security Risk Management, Audit Report No. 44, 2008-09*, Australian National Audit Office, Canberra, viewed 20 January 2016, http://www.anao.gov.au/uploads/documents/2008-09_Audit_Report_44.pdf

Australian Institute of Criminology 2014, *Australian crime: Facts & figures 2013*, Australian Government, Canberra, viewed 20 January 2016, http://aic.gov.au/publications/current%20series/facts/1-20/2013.html

Borzycki, M & Fuller, G 2014, *Armed robbery in Australia 2009-10: National Armed Robbery Monitoring Program report*, Australian Institute of Criminology, Canberra, viewed 20 January 2016, http://www.aic.gov.au/publications/current%20series/mr/21-40/mr22.html

Brooks, DJ 2011, 'Security risk management: A psychometric map of expert knowledge structure', *Edith Cowan University Publications*, viewed 20 January 2016, http://ro.ecu.edu.au/ecuworks2011/34/

Comcare, 2009, *Cash in transit*, Australian Government, viewed 20 January 2016, http://www.comcare.gov.au/Forms_and_Publications/publications/services/fact_sheets/fact_sheets/cash_in_transit/cash_in_transit

Cornish, DB & Clarke, RV 2003, 'Opportunities, precipitators, and criminal decisions: A reply to Wortley's critique of Situational Crime Prevention', *Crime Prevention Studies*, vol. 16, pp. 41-96.

Crime Prevention NSW 2014, *Fact sheet: Designing crime out of your business*, New South Wales Department of Justice, viewed 20 January 2016, http://www.crimeprevention.nsw.gov.au/Documents/business_security_factsheet_oct2014.pdf

Fuller, G 2014, *Where and when: A profile of armed robbery by location*, Trends & issues No. 479, Australian Institute of Criminology, Canberra, viewed 20 January 2016, http://aic.gov.au/publications/current%20series/tandi/461-480/tandi479.html

Goetschel, L 2000, 'Globalisation and security: The challenge of collective action in a politically fragmented world', *Global Society*, vol. 14, no. 2, pp. 259-277, http://www.academia.edu/5677535/Globalisation_and_Security_The_Challenge_of_Collective_Action_in_a_Politically_Fragmented_World

Industrial Relations Commission of New South Wales 1997, *Matter No. IRC 1880 OF1995 Reference by the Minister for Industrial Relations the Transport and delivery of cash and other valuables industry*, Industrial Relations Commission of New South Wales.

Isotalo, J n.d, 'Basics of Statistics', *Lecture notes University of Tampere*, Finland, viewed 20 January 2016, http://www.mv.helsinki.fi/home/jmisotal/BoS.pdf

Morgan, A, Boxall, H, Lindeman, K & Anderson, J 2011, *Effective crime prevention interventions for implementation by local government*, AIC Reports Research and Public Policy Series 120, Australian Institute of Criminology, Canberra, viewed 20 January, http://aic.gov.au/publications/current%20series/rpp/100-120/rpp120.html

NSW Police Force, n.d, *Frequently Asked Questions*, Security Licensing & Enforcement Directorate ,viewed 23 January 2016, https://www.police.nsw.gov.au/services/security_licensing_and_enforcement_directorate/security_licences/renew_online/?a=7474#TRAINING

Office of Regulatory Services 2012, *Security Industry Licensing Practice Manual*, Australian Capital Territory Government, Canberra, viewed 20 January 2016, https://www.accesscanberra.act.gov.au/ci/fattach/get/47716/1435895098/redirect/1/filename/Security%20industry%20licensing%20practice%20manual.pdf

Parliament of New South Wales 1997, *Security Industry Act 1997 No 157*, Parliament of New South Wales, viewed 20 January 2016,

http://www.legislation.nsw.gov.au/inforcepdf/1997-157.pdf?id=a960831c-d892-c958-9131-b7a769043f7d

Queensland Government 2015, *Premises security planning and crime prevention*, Business and Industry Portal, viewed 20 January 2016,

https://www.business.qld.gov.au/business/starting/business-premises-utilities/premises-security-and-crime-prevention/premises-security-planning-and-crime-prevention

Rudd, K 2008, *The First National Security Statement to the Australian Parliament*, Department of Prime Minister and Cabinet, viewed 10 November 2010,

http://pmrudd.archive.dpmc.gov.au/node/5424

Security 2014, *Merriam-Webster's online dictionary*, viewed 20 January 2016,

http://www.merriam-webster.com/dictionary/security

Smith, L & Louis E 2010a, *Armed robbery in Australia: 2007 National Armed Robbery Monitoring Program annual report*, Australian Institute of Criminology, Canberra, viewed 20 January 2016, http://www.aic.gov.au/publications/current%20series/mr/1-20/11.html

Smith, L & Louis E 2010b, *Cash in transit armed robbery in Australia*, Trends & issues No 397, Australian Institute of Criminology, viewed 20 January 2016, http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi397.html

Smith, L, Louis, E & Preston L 2009, *Service station armed robbery in Australia, Trends and issues No. 373*, Australian Institute of Criminology, viewed 20 January 2016, http://www.aic.gov.au/publications/current%20series/tandi/361-380/tandi373.html

Standards Australia/Standards New Zealand 2009, *AS/NZS ISO 31000:2009 Risk management-principles and guidelines,* Standards Australia/Standards New Zealand, Sydney Australia.

Standards Australia/Standards New Zealand 2006, *HB 167:2006 Security Risk Management*, Standards Australia/Standards New Zealand, Sydney.