Processed based approach to Critical Infrastructure Protection: Using a proactive security management process.

W. J. Bailey. Edith Cowan University, Australia

Adopting a ‘Processed’ approach attempts to more formally structure how using the normal risk based approach needs to be enhanced to include a wider range of considerations, including vulnerability and threats, as well as incorporating a more systematic way to make sure it is a comprehensive methodology. Basically it is a flow-chart of what needs to be done each time, and repeated on subsequent assessments or when change occurs in any of the criteria.

The function of security in business is a supporting role to allow business to continue to operate safely, securely and be commercially viable. The more hostile the environment the more important this role becomes. When it is necessary to protect critical infrastructure the role of security becomes essential; as potential loss or destruction can have catastrophic consequences not only for business, but for the society generally. Therefore, the role of security becomes more focussed on prevention, as failure is not an option In order to ensure this aim is achieved, all the threats need to be considered, assessed and are duly covered in a systematic processed approach. The fundamentals of security remain: detect, delay, deny, deter, defend and respond. (Marier, 2012, Brooks, 2014; Ezell, 2007)

The ability to develop an operational security management plan is dependent on accurately assessing the threat, risks and capability of adversaries to impact on the working environment (Garcia, 2006). Extensive background information needs to be obtained from a number of sources in order to produce a Security Risk and Threat Assessment (SRVTA) (Bailey, 2013). To be effective in this task requires an understanding of how grave the problem is, and in which specific areas, before any meaningful action can be taken. Therefore, undertaking a comprehensive security, risk and threat assessment is necessary to fully understand the nature and scope of the problem first.

A Security Risk Assessment requires an all-inclusive understanding of the social, economic and political factors before successful and meaningful security managed programmes can be implemented or even suggested. (Andersen, 2014;World Bank, 2014).

The key to achieving the required level of protection is awareness of what constitutes a threat, is vulnerable and therefore a risk. Setting an established well-defined series of systems and processes to monitor ongoing risks and dealing with them accordingly are part of this key.

This paper is based upon personal experience of working in the oil and gas industry predominately in hostile environments in Africa and Papua New Guinea. It has been developed and written up over a number of years in various conference papers and chapters in books. Two of the most recent are:

(Bailey, 2016) Bailey, W. J. (2016**). Protection of Critical Homeland Assets: Using a Proactive, Adaptive Security Management Driven Process**. In M. Dawson, Kisku, D. R., Gupta, P., Sing, J. K., & Li, W. (Ed.), *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 394). Hershey, PA: IGI Global.

(Bailey, 2013) Bailey, W. J. (2016). **Protection of Critical Homeland Assets: Using a Proactive, Adaptive Security Management Driven Process**. In M. Dawson, Kisku, D. R., Gupta, P., Sing, J. K., & Li, W. (Ed.), *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 394). Hershey, PA: IGI Global.

Consequently, for a more detailed description of the processes briefly described in this paper are laid out in these publications.

The question asked in this conference is: "What is best, a Risk based or Process Based approach?"

Risk is a probabilistic concept based upon the notion that it is possible to make an informed selection of future events based upon previous outcomes as a likelihood they will occur again or at the very least are estimable with a reasonable degree of consistency. By the creation of probability as a concept, added to by the development of mathematical determination of such probability the assumption is made that it is possible to identify how likely it is for an event to happen. (Bernstein, 1996). Risk at its very best is subjective and cannot never be definite only probable: it may or may not happen.

Nonetheless, based upon this thesis a whole industry has evolved professing to be able to foresee the future. Unfortunately, we know this is not possible and many a situation has occurred which was deemed to be impossible or unlikely to happen within a 1000 years or greater: yet did! There have also been many attempts to create a risk matrix based upon the multiplication of numbers such as *probability x consequence* in an attempt to synthesise "the findings in easy-to-grasp tables, where identified risks are assessed as numerical indexes (sic)- listed as easily understandable and comparable numbers-and prioritised"(Manunta, 2002).

Many multinationals have attempted to adopt this method for risk assessment in misguided belief it reduces the likelihood for error and can be easily accomplished by a computer programme or a simple apt. When dealing with Security and Safety this approach is not acceptable; especially where a loss of life is a distinct probability. However, based upon experience infused with subjectively, it is possible to manage potentially dangerous and hostile situations if the right approach has been taken to fully comprehend, mitigate and deal the risks. A systematic risk based approach is required to identify the potential hazards, the probable threats and how to deal with them founded upon a full understanding of the likely consequences. Consequence thus becomes the key identifier for establishing what is critical and therefore in need of substantial protection (Bailey, 2016).

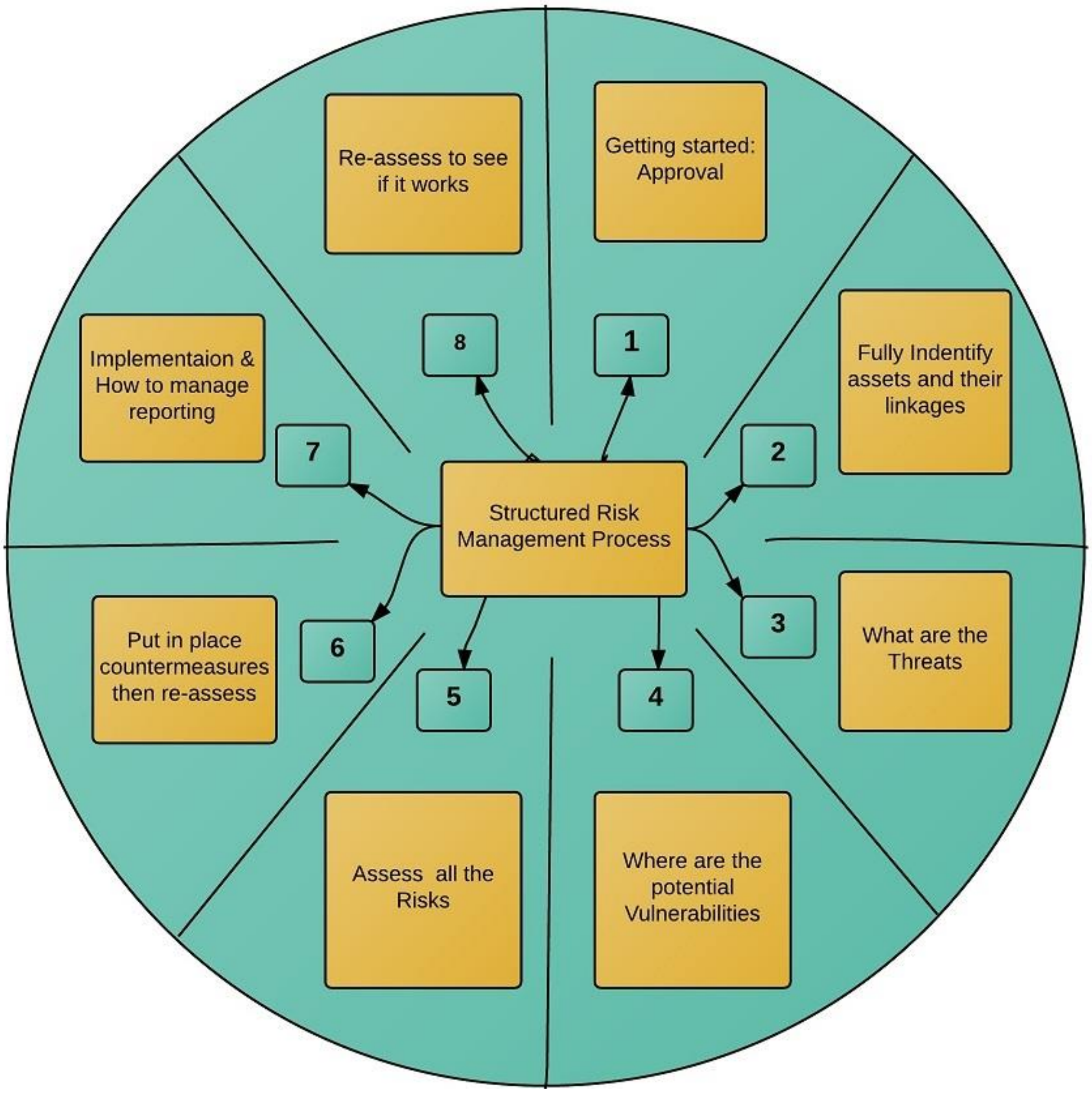

Structured Risk Management Process
1
Getting started: Approval
2
Fully Indentify assets and their linkages
3
What are the Threats
4
Where are the potential Vulnerabilities
5
Assess all the Risks
6
Put in place countermeasures then re-assess
7
Implementaion & How to manage reporting
8
Re-assess to see if it works

Figure 1 The risk assessment process consists of sequential sub-elements

The Risk Assessment process consists of sequential sub-elements:

- Understand the context,
- Identify the risks,
- Analyse the risks,
- Evaluate the risks,
- Assess the potential threats,
- Fully understand the consequences,
- Identify and evaluate the existing risk controls,
- Implement protection with robust resiliency measures,
- Constantly evaluate the measures assessing further risk treatments and opportunities for improvement,
- Communicate, consult, monitor and review. (Standards Australia, 2009)

The use of a structured, more adaptive and proactive security management process increases the robustness of any proposed mitigation measures to be put in place. By adopting these tried and tested measures into security management more generally, the protection of assets within critical infrastructure can be greatly improved upon. The necessary objective is to develop effective, efficient, safe and legally realistic strategies to deal with the risks. “The ultimate goal of each strategy is to transform unacceptable into acceptable”(Klinke & Renn, 2002, p. 1085).

A key element of Security Risk Management, that distinguishes it from other forms of risk management, is that the risk management process is often separated in practice into two elements - a Security Risk Assessment and Security Risk Management. (Talbot, 2009)

The role of risk management is to establish and protect valued assets.

> Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation. (Standards Australia, 2013)

The crucial objective when dealing with risks, which are considered not to be acceptable to the risk appetite of the company or organisation , is to convert the risks to tolerable and consequently more acceptable in terms of potentially negative outcomes. This can be achieved through adopting alternative measures that mitigate the risk. However, for this process to be conducted in a productive manner ‘Consequences’ have to be made central to the whole risk management process.

Only by fully understanding what the consequences would be to the whole operation or organisation, can any meaningful risk elimination or mitigation measures be adopted.

Understood from a safety perspective, one which most large organisations have now incorporated into the security management structure, the first line of defence is to engineer the risk out by eliminating it completely. Unfortunately, this is not always practical or affordable, but every effort should be made to achieve this desired objective: elimination. For example, rather than moving vital personnel through hostile and dangerous environments by road, consider flying them.

Understand what are often called the risk triplets: scenario, probability and consequences

i. What can happen ? (i.e. What can go wrong?)
ii. How likely is that will happen?
iii. If it does, what are the consequences? .(Kaplan, 1981)

Comprehending what are the likely negative outcomes thus becomes essential if this risk is to be dealt with appropriately. This why a systematic methodology is developed by building a table with all the scenarios together with outcomes coupled with mitigation measures.

Furthermore, it is important to recognise that the ‘supply chain’ forms part of the vulnerability as much as the asset itself and should therefore also be reflected in the consequences (George, 2015). Failure to fully assess the potential problems of replacement or rebuild, including time constraints, could further exasperate a serious incident into a major or calamitous one. Therefore, impact is not the same as consequences: they are similar, but should be considered as two separate aspects. Impact is what happens first. Consequences or outcomes are those that are related to the impact, but could have progressively damaging effects on the event. (Bailey, 2016)

The central theme utilised to provide a reliable and robust Risk Management matrix lies within AS/NSZ ISO 31000:2009 (Standards Australia, 2009). The Standard provides a common multiple over layering foundation upon which risk management protocols can be built. The generic attributes of ISO 31000 permits any organisation to undertake the risk process if they follow the process. Risk Management creates and protects value and “how to take account of the mix of facts, uncertainties, perceptions, complexities, beliefs and values when taking decisions about risk”(Standards Australia, 2010).

In order to perform a substantive assessment of the risk an adaptive, proactive model becomes essential and is termed the Security, Risk, Threat and Vulnerability Assessment (SRTVA). By adaptive we mean capable of being flexible, responsive and able to evolve dependent on the circumstances. Proactive requires a non- passive approach to threats and risks. Furthermore, as threats are asymmetric they require a subjective approach to incorporate them into the holistic model that needs to be created. .Only by adopting the initiative can a pre-emptive strategy be put into place .

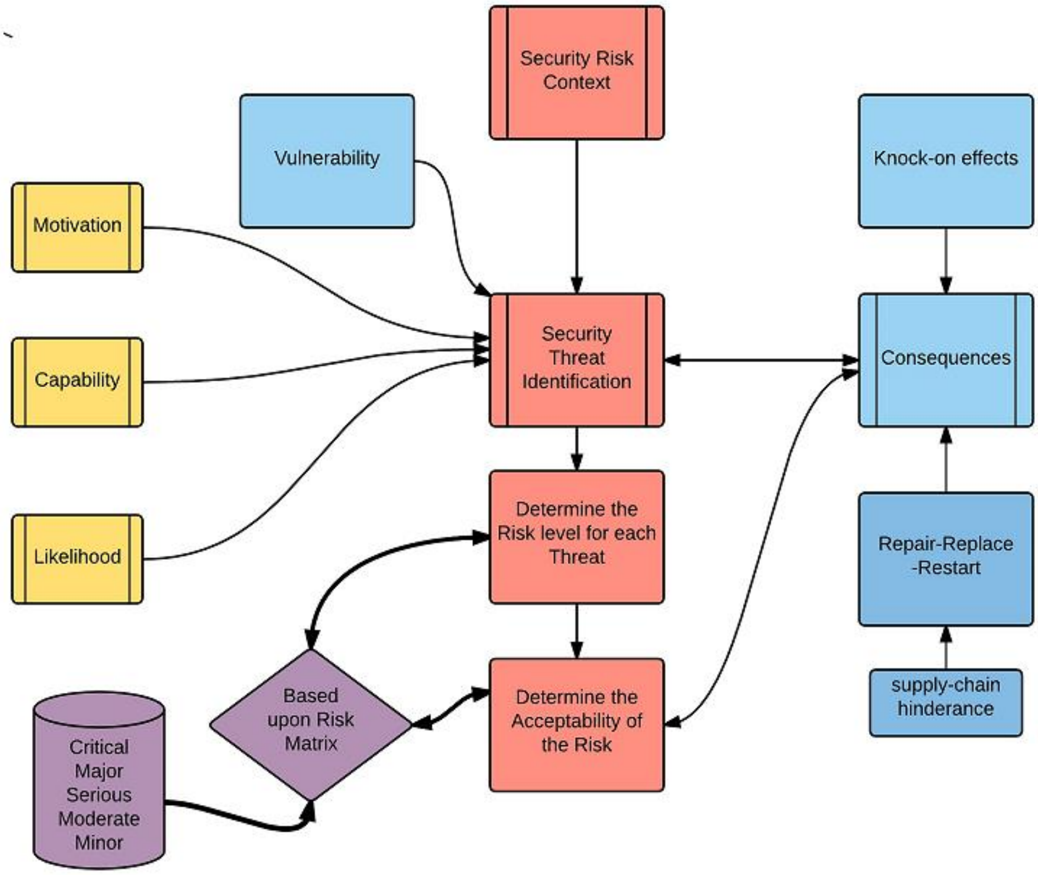


Figure 2 Consequence considerations (Bailey, 2016)

The fundamental aspect related to potential negative outcomes and consequences drives the SRVAT process. Only by fully understanding this relationship can it be hoped to achieve an operational mechanism by which risk can be dealt with satisfactorily. A SRVT assessment is far more comprehensive than many managers appreciate as:

> security is only one facet of risk and therefore must be considered in the context of holistic risk management across the enterprise, along with other categories such as market, credit, operational, strategic, liquidity and hazard risks.(Garcia, 2006)

Only by taking this holistic approach can all the risk scenarios be captured and thus dealt with effectively. (Brooks, 2014). In addition, not only must the negative outcomes be assessed they must also be considered in how long will it take to repair, replace and restart operations. When this is considered for some areas a new factor is brought into the process and this is the supply-chain- hindrance. Whereby obtaining replacement parts is prohibitive and problematic; especially in remote and hostile locations.

Undertaking a SRVTA is best undertaken with a team made up of key stakeholders and managers from the various organisation. However the team must be led by a highly trained and experienced security management professional. Often untrained people have been used to carry out the risk management for security operations. In most cases this happens as there is confusion over a risk analysis used for health and safety, and one required for security. The principals are similar, but security must consider threats and vulnerability as well. The preferred option is to have a team that is made up of specialists from different disciplines whom fully understand the operational requirements of the organisation. The team should always include a senior health and safety specialist as the assessment proposals will need to be accepted at the highest level, which must always include elements of health and safety. It will then be possible to accurately identify what is in fact critical giving it an identifier in the criticality matrix.

By undertaking the SRTVA, as a team, the outcomes will have greater validity with senior management as it reflects a combined approach, rather than a single individual from the security department. (Boeing et al, 2008) By incorporating other areas a more holistic understanding of operations can be accomplished. “the degree of consensus among key stakeholders is one of the key drivers for selecting the right management strategy”. (Abrahamsen, 2015)

The Role of Intelligence

One area that needs to be added to every security risk assessment process is the inclusion of intelligence data. No SRVTA can achieve the desired results without input and information from a multitude of sources, which are collectively known as intelligence. The collection, collation and processing of this type of information is a fundamental process normally associated with warfare, but now forms an integral part of national security, foreign policy, law enforcement and the broader areas involving government activities: such as protection of critical infrastructure. Nowadays, intelligence is an essential aspect of business activity involving all sections of the organisation, used in order to develop and hone strategies (Herring, 1992). Business espionage has become highly developed worldwide, as gaining knowledge of competitor's technical data is greatly sought after.

In 2006 Treaty negotiators between Australia and East Timor over the international sea boundary negotiations Australian foreign intelligence agents bugged the cabinet rooms in Dilli to get the upper hand in negotiations.

> "We were not aware at the time, that under the cover of an Australian program renovating Timor-Leste government offices, Australia installed listening devices to spy on the Timorese officials," Minister of State Agio Pereira said, "To maximise their advantage and commercial interest."(Cannane, 2016)

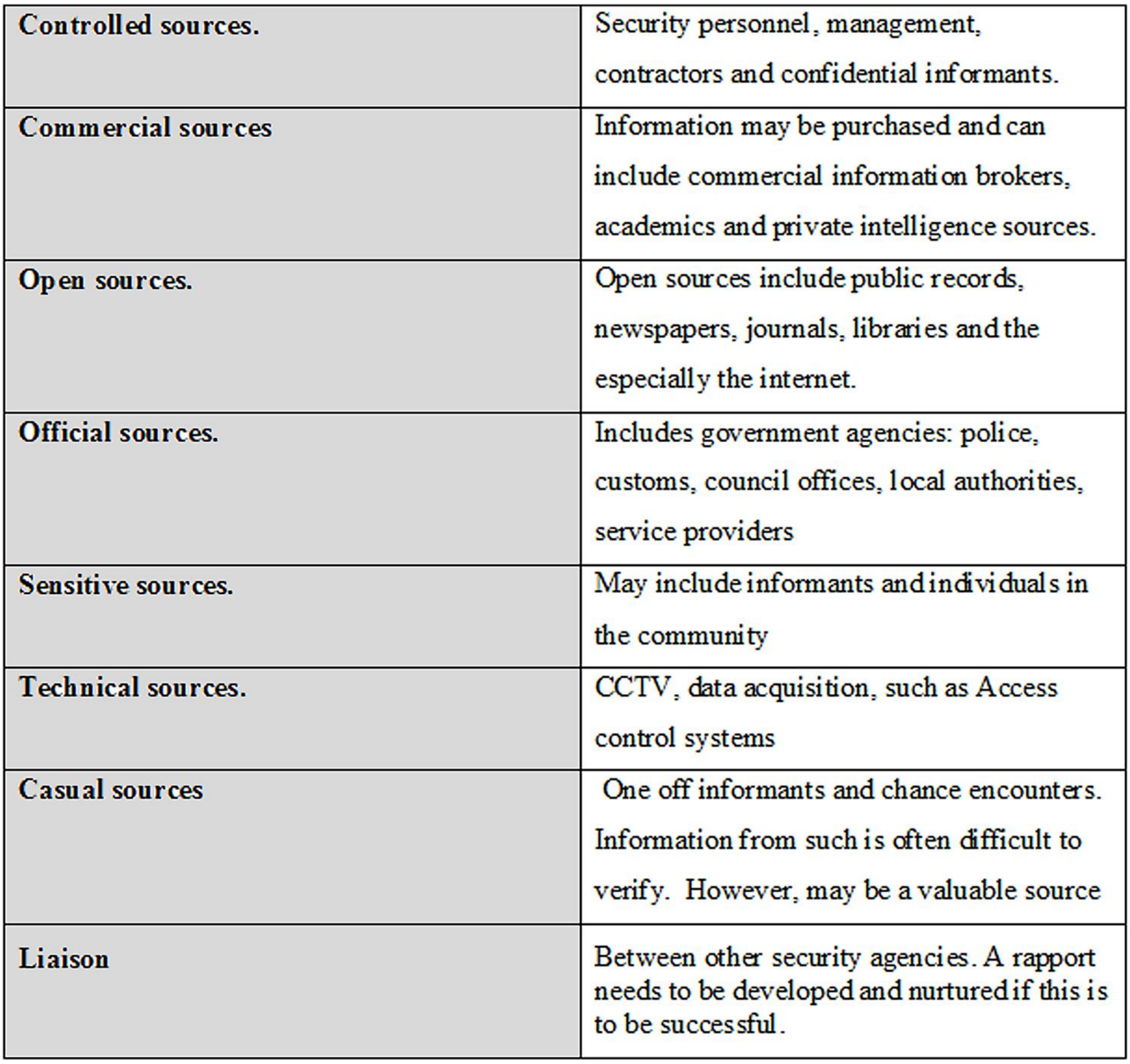
In order to make effective business decisions comprehensive knowledge of competitors activities is desirable. Therefore, obtaining useful intelligence is essential to conducting a worthwhile SRVTA. Intelligence describes both a product and a process. (Bailey, 2016)

> Intelligence is the umbrella term referring to the range of activities – from planning and information collection to analysis and dissemination – conducted in secret, and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventative policy or strategy, including, where desirable, covert activities. (Gill, 2006)

Coordinating and sharing intelligence gathered has and still is one of the more difficulty areas to rectify as most government agencies are very protective of their data. This was immediately recognised post 9/11 in the United States which led to the creation of the Department of Homeland Security in March 2003, Initiated by the passage of the Homeland Security Act of 2002 (Perrow, 2006; Lewis, 2006; Moynihan, 2005; Relyea, 2003; Mueller, 2016). Other countries have followed the lead of the USA and tried to make their agencies more 'joined-up' and allow intelligence sharing. Nonetheless, obstacles still hinder progress to fully benefit the protection of critical assets with time constant intelligence.

The intelligence cycle involves developing priorities and strategies for the process of collection dependant on the priorities. Following collection comes the important aspect of analysis, often considered the most difficult, as those charged with analysis need to be aware of what aspects are important. Have the right questions been asked in the first place? Very often vital pieces are missed as they were not thought important enough to include in the reports that are moved up to decision makers. Strategy and policy can only be made based upon substantiated data, or an analysis of what the data might mean in the way of threats. Although ‘Intelligence failure’ is sometimes used as an excuse for attacks, this would be unjust as it impossible to have accurate intelligence all time, or for decision-makers to understand fully the implications of what the analysis has interpreted as a likely outcome (Taylor, 2007).

Table 1 Sources of intelligence (Bailey, 2016)



Controlled sources.	Security personnel, management, contractors and confidential informants.
Commercial sources	Information may be purchased and can include commercial information brokers, academics and private intelligence sources.
Open sources.	Open sources include public records, newspapers, journals, libraries and the especially the internet.
Official sources.	Includes government agencies: police, customs, council offices, local authorities, service providers
Sensitive sources.	May include informants and individuals in the community
Technical sources.	CCTV, data acquisition, such as Access control systems
Casual sources	One off informants and chance encounters. Information from such is often difficult to verify. However, may be a valuable source
Liaison	Between other security agencies. A rapport needs to be developed and nurtured if this is to be successful.

Using New Technology

The main objective of the SRVTA is the protection of critical and valuable infrastructure Trying to identify what is in fact ‘critical’ sometimes proves to be very difficult as threats constantly evolve. An interactive prototyping tool can be useful in playing out scenarios and simulating the effect of any changes that may be proposed, however existing simulators in the critical infrastructure area are typically limited in their visual representation and interactivity.

To remedy this, the use of games technology is proving to be useful as it allows for an interactive simulation. Critical infrastructure scenarios can be rapidly constructed, tested, and refined.

> Simulation unambiguously represents the importance of understanding the realities of ‘consequence’ in the overall security risk mitigation process. It becomes more obvious because of the visualisation process. Being able to see what went wrong makes it easier to put it right. Appreciating the nature of the actual consequences also helps in ascertaining what needs to be done to rectify the weakness. In addition, a cost-analysis-benefit can be performed assessing the outlay involved in comparison with other feasible mitigation strategies. (Boeing et al, 2008)

Throughout this paper emphasis has been place on the role of consequences in the SRVTA assessment process. This emphasis cannot be highlighted too often especially when dealing with critical infrastructure. Failure to fully comprehend potential negative outcomes sufficiently, and take the appropriate counter-measures, exposes the nationals assets to attack, damage and destruction.

Therefore, once the SRVTA has been fully completed a meeting should be conducted with major stakeholders. The observations, recommendations and conclusions developed during the assessment process should be fully discussed and include the following:

- Provide a summary of the Threat Characterization Statement;
- Discuss the current effectiveness of the safeguards and security program; including a register of any gaps in the baseline countermeasures;
- Provide an overview of the risk assessment, reviewing all recommendations contained in the audit report;
- Establish responsivities for the implementation, timing and review of the SRTVA report.

After the SRVTA analysis is complete, the risk and vulnerabilities can should be resolved by deciding to:

- accept the risk associated with the vulnerability,
- eliminate it completely or
- control the source of the vulnerability.

Mitigation can take on many forms as cost and practicality are part of the equation. The elimination of the vulnerability remains the ultimate objective. (W.J. Bailey, 2016, p. 40)

Conclusion

The thrust of this paper has been to promote the idea of adopting a far more comprehensive security management methodology when it comes to protecting critical infrastructure. By combining a far more wide-ranging series of procedures into a single methodology allows the protection of critical infrastructure to move from response based mode to a more proactive and adaptive mode. Move from merely fire-fighting by taking the initiative to act first and forestall potential breaches to critical infrastructure security. Furthermore, it pushes the purpose of the assessment to look harder at the potential consequences and what these could actually mean if they occurred. Too often lip service is given to what may happen with nothing is done to protect the assets rather than dealing with potential costs head on.

In addition, the proactive and adaptive security management process is a holistic process, which also needs to be based upon sound intelligence gathering capabilities and effective dissemination systems. The objective is to identify threats, vulnerabilities and consequences from a security perspective and treat them accordingly. Adding and developing additional supporting mechanisms: including red-teaming, desk-top exercises, real time test penetration of facilities and particularly those being developed by new technology such as computer based modelling. Rapid developments in security technology are likely to produce far more effective methods of improving and strengthening security.

Therefore, in answer to the question posed: the risk based approach needs to be built upon to make it more robust by adding more to the process; it is not either or!

References

Abrahamsen, E. B., Pettersen, K., Aven, T., Kaufmann, M., & Rosqvist, T. (2015). A framework for selection of strategy for management of security measures. *Journal of Risk Research*, 1-14. doi:10.1080/13669877.2015.1057205

Andersen, T. J., Garvey, M., & Roggi, O. (2014). *Managing risk and opportunity: The governance of strategic risk-taking*: Oxford University Press.

Bailey, W. J. (2016). Protection of Critical Homeland Assets: Using a Proactive, Adaptive Security Management Driven Process. In M. Dawson, Kisku, D. R., Gupta, P., Sing, J. K., & Li, W. (Ed.), *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 394). Hershey, PA: IGI Global.

Bailey, W. J., & Doleman, R. (2013). Proactive security protection of critical infrastructure: A process driven methodology. In C. Laing, A. Badii, & P. Vickers (Eds.), *Securing critical infrastructures and critical control systems: Approaches for threat protection*. Hershey, PA. : IGI. Publishers.

Bernstein, P. L., & Bernstein Peter, L. (1996). *Against the gods: The remarkable story of risk*: Wiley New York.

Boeing, A., Masek, M., & Bailey, B. (2008). Protecting critical infrastructure with games technology. *School of Computer and Information Science, Edith Cowan University, Perth, Western Australia*(9th Australian Information Warfare and Security Conference).

Brooks, D. J., & Smith, C.L. . (2014). Engineering principles in the protection of assets,. In M. Gil (Ed.), *Handbook of Security* (pp. 107-132). London, England: Palgrave Mcmillian.

Cannane, S. (2016). East Timor says Australia took advantage of a vulnerable nation, demands Timor Sea treaty torn up. *ABC News*. http://www.abc.net.au/news/2016-08-30/east-timor-demands-timor-sea-treaty-torn-up/7797118

Ezell, B. C. (2007). Infrastructure vulnerability assessment model (I VAM). *Risk Analysis, 27*(3), 571-583.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Burlington, MA: Elsevier Butterworth-Heinemann.

Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world*. London, England: Polity.

Herring, J. P. (1992). The role of intelligence in formulating strategy. *Journal of Business Strategy, 13*(5), 54-60.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11-27.

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*. Monterey, CA: John Wiley & Soms.

Manunta, G. (2002). Risk and Security: Are they Compatible Concepts? *Security Journal, 15*(2), 43-55. doi:10.1057/palgrave.sj.8340110

Marier, K. (2012). The 5 D's of Outdoor Perimeter Security. *Security, 49*(3), 64-64.

Moynihan, D. P. (2005). Homeland security and the US public management policy agenda. *Governance, 18*(2), 171-196.

Mueller, J., & Stewart, M. G. (2016). *American public opinion on terrorism since 9/11: Trends and puzzles.* Paper presented at the National Convention of the International Studies Association,, Atlanta, Gr.

Perrow, C. (2006). The disaster after 9/11: the department of homeland security and the intelligence reorganization. *Homeland Security Affairs, 2*(1).

Relyea, H. C. (2003). Organizing for homeland security. *Presidential Studies Quarterly*, 602-624.

Standards Australia. (2009). AS/NZS ISO 31000:2009. Risk management *Principles and guidelines: In context*. Australia: Standards Australia International Ltd.

Standards Australia. (2010). HB 327: 2010 *Communicating and consulting about risk: Companion to AS/NZS ISO 31000:2009*. Sydney, Australia: Standards Australia, International Ltd.

Standards Australia. (2013). SA/SNZ HB 436:2013 (Guidelines to AS/NZS ISO 31000:2009) *Risk management guidelines - Companion to AS/NZS ISO 31000:2009*. Sydney, Australia: Standards Australia International Ltd.

Talbot, J., & Jakeman, M. (2009). *Security risk management: Body of knowledge*. London: John Wiley & Sons, Inc.

Taylor, S. A. (2007). The role of intelligence in national security. *Contemporary security studies*, 250.

World Bank. (2014). *Risk management can be a powerful instrument for development*. Retrieved from Washington, DC: http://elibrary.worldbank.org/doi/abs/10.1596/9780821399033_Ch01