2008

The risk intelligence conundrum and its impact on governance

Mark Loves
University of Wollongong

The risk intelligence conundrum and its impact on governance

Abstract

This paper looks at intelligence led strategic planning, specifically within the context of an operational private sector corporate security unit which the author managed from 1994 to 2005. It examines the role, mission and objectives of the unit, with specific emphasis on management models, planning frameworks, policy and strategy, client relations and performance measuring. It develops the concept that risk assessment and intelligence development are in fact the same process, acting to direct governance and informing decision making at both tactical and strategic levels.

Disciplines

Law

Publication Details

M. F. Loves, "The risk intelligence conundrum and its impact on governance" in K. Michael & M. G. Michael(ed), Australia and the New Technologies: Evidence Based Policy in Public Administration (2008) 24-31.

5

The risk intelligence conundrum and its impact on governance

Mark Loves*
Senior Lecturer, Program Manager, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

This paper looks at intelligence led strategic planning, specifically within the context of an operational private sector corporate security unit which the author managed from 1994 to 2005. It examines the role, mission and objectives of the unit, with specific emphasis on management models, planning frameworks, policy and strategy, client relations and performance measuring. It develops the concept that risk assessment and intelligence development are in fact the same process, acting to direct governance and informing decision making at both tactical and strategic levels.

Keywords: intelligence, strategic planning, compliance, risk management, risk intelligence, value chain model, value network model, value workshop model, internal consultancy model, client relations, performance measurement

1 Introduction

In any paper on intelligence, it becomes necessary to define the term, as there is the potential for confusion surrounding its meaning. Intelligence, as it is applied in a national security context is a process, defined by its components which are popularly categorised as planning, collection, collation, analysis and dissemination. However the term intelligence is also used to describe the end product of that process, as well as defining organisations or groups that carry out the various functions involved in the process (Lowenthal, 2006). For the purpose of this paper, intelligence is defined by its process, which is designed to add value to information and ultimately focused on assisting policy makers in their decision making.

Within traditional law enforcement and national security, intelligence has traditionally been regarded as an operational, strategic or tactical driver. However, with ever increasing demands on organisational efficiency and effectiveness, intelligence is now being promoted as a formal basis for strategic business planning (Christopher, 2004). In this context the intelligence function or what intelligence is used for, involves the proactive interpretation of the business environment. It has at its core the ability to respond flexibly to situations to manage risks, take advantage of fortuitous developments, make sense of contradictory information and ensure efficient and effective results from operations and strategies (Grieve, 2004). Ultimately, intelligence is used to inform decision making at the tactical and strategic levels and is designed to act as a guide to managing operations (Ratcliffe, 2004).

In contrast, traditionally risk has been used to describe the chance of something happening that will impact upon the achievement of organisational objectives. Risk assessment as a process, is based on a measurement of impact and probability. It derives from notions of capitalism, religious turmoil and scientific vigour born of the French Renaissance period, when probability theory was transformed from a "gamblers toy" to a method of predicting and benefiting from the future based on the organisation, analysis and interpretation of available information. This transformation is described by Bernstein as the beginning of the theory of decision making, "deciding what to do when it is uncertain what will happen" (Bernstein, 1998). Upon consideration, this mix of limited information, uncertainty and decision making bears startling similarity with the intelligence process and functions.

This paper looks at the issue of strategic planning within the context of an operational private sector corporate security unit and examines how the role, mission and objectives of the unit drive the development of strategy and policy through risk assessment. It also examines similarities within the disciplines of risk and intelligence and draws conclusion on their interdependence within an overarching framework of governance modelling.

2 Management model

Management is regarded as the process of coordinating work activities so that they are completed with and through other people, in the most efficient, "doing things right" and effective, "doing the right things" way (Robbins, Bergman, Stagg & Coulter, 2006). Whilst there are numerous management models, consensus is that they are generally derivations on three critical management functions; planning, (defining goals, establishing strategy and developing plans), organising (arranging work to accomplish goals) and controlling (evaluating whether things are going as planned) (Robbins et al. 2006; Rogers, Ure & Young, 2007; Stoner, Collins and Yetton, 1985).

In strategic planning, intelligence is critical in assessing client expectations and selecting which management model is best suited to the role, mission and objectives of the unit. Intelligence also impacts upon management modelling, as it can provide performance feedback which may reflect on the adequacy of the model. Intelligence therefore can act as a catalyst for change or amendment to the management model.

2.1 Role, Mission and Objectives

Within the corporate security unit, the role, mission and objectives were established at the planning stage of the management model (diagram 2), although they had real implications for both the organising and controlling stages. The unit's role was to support the company in achieving its corporate objectives, being the maintenance of profitable operations through effective utilisation of its critical infrastructure and resources. Its mission was the identification and protection of those critical assets and infrastructure most responsible for assisting the company achieve its corporate objectives. The unit's objectives related to the efficient and effective establishment and implementation of infrastructure, physical asset, information (logical, intellectual and hard copy), personnel and financial security risk plans, to protect the assets thus identified and to provide business continuity in the case of catastrophic

loss (Broder, 2000). To achieve these objectives, the author devised and implemented the management model (diagram 1), which also acted as a governance framework.

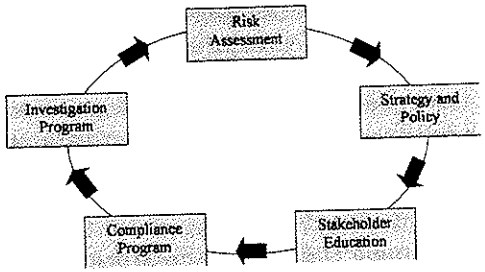

Diagram 1. Corporate Security Unit risk based governance framework

3 Management planning framework

Rogers et al. (2007) describe several models within management planning frameworks. The Value Chain Model describes the process of producing consumer goods from raw materials. The Value Network Model matches client needs with services offered, to mutual advantage. The Value Workshop Model involves the client being treated as the focus of attention, where the only identifiable output is the client's satisfaction. Finally, the Internal Consultancy Model focuses on delivering products and services that can't be obtained elsewhere.

In the author's experience within policing, security and intelligence agencies, the Value Workshop and Consultancy Models were predominantly utilised. Within the corporate security unit, a similar consultative risk based management planning framework was utilised [diagram 1], involving risk assessment, developing policies and strategies to address unacceptable risks, education programs, (to educate decision makers and other stakeholders on those risks, strategies and policies), compliance programs (to ensure stakeholder implementation), and where control failures were identified, investigative programs to identify cause and develop remedy. This whole process then fed back into the risk assessment phase and the model would commence again.

Intelligence considerations played a dominant role in the development of this framework with its major emphasis on risk assessment (intelligence development) as the core of the management model. To demonstrate the risk/intelligence relationship, the author developed comparative modelling to demonstrate to the company (client) how intelligence overlaid the risk management process (diagram 2). In this model, the risk management and intelligence functions are complementary, if not the same process however, it's not so much the governance framework contributing to the intelligence function as it is the intelligence function driving the framework. Apgar (2008) describes a similar process in using the example of telecommunications company AT&T, in observing that the company's inability to understand its capacity for taking risks led to a too cautious approach to the introduction of broadband Internet services in the 1990's, a policy decision which ultimately led to its financial detriment. In this context, he interprets risk intelligence as "our ability compared to competitors to assess a risk".

The first step in the management planning framework was a consultative organisational security risk assessment (diagram 1). This assessment was initially conducted as a series of site visits, observations and interviews with internal and external stakeholders (including senior executives). Information was also gathered from industry benchmarks, statistical incident and insurance data bases, agency reports, internal / external audit and industry experts. Comparative analysis was then conducted across the information to develop risk intelligence. The aim of this risk intelligence process was to:

- identify those assets, personnel, information, processes and systems (including financial) which were most critical to the Company in achieving its corporate objectives,
- identify the major security risks to those critical assets, and
- assist in identifying potential policy and strategy that would assist in protecting those critical assets.

The model met three major criteria for the successful use and management of intelligence within organisations (Rogers, et al. 2007). It provided an upward organisational focus (risk assessment, policy and strategy) where intelligence was emphasized as a means for achieving the goals of the company. It provided a downward focus to ensure that these organisational priorities were understood and implemented by the work force (education and compliance) and it provided a facility to identify and address issues and non performance at an early stage ("focus on self") at the investigation phase.

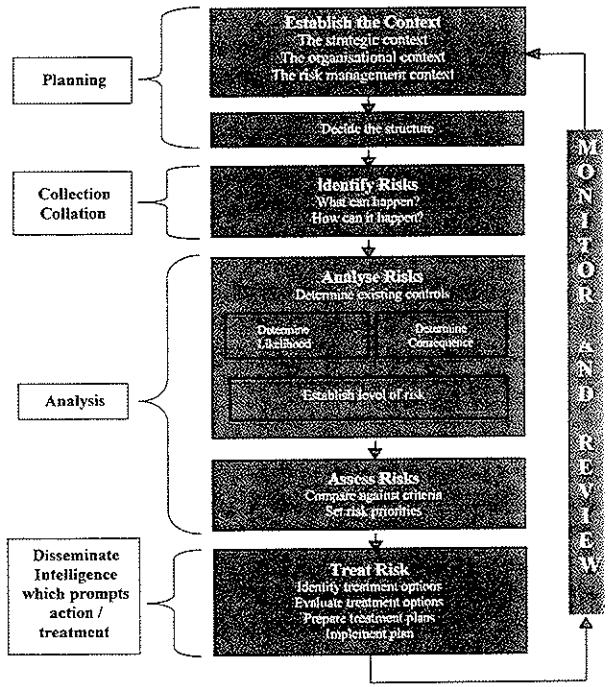

Diagram 2. The relationship between intelligence and risk management
(Based on AS/NZS 4360:2000 - Risk Management) – (Loves, 2000)

4 Policy and strategy

There appears to be no universally accepted definition of strategy. Mintzberg and

Quinn (1991) described it as a pattern, ploy, plan or position that integrates organisational goals into a cohesive whole, which deals with the "*unpredictable and unknowable*". Maister (1997) described strategy as finding new ways to do things, or an improvement in core business requiring changes in behaviour. Yarger (n.d.) agrees that strategy is a general plan or course of action which is both proactive and anticipatory, but goes further to describe it as hierarchical (cascading from top level down), comprehensive (considers the whole of the strategic environment) and developed through analysis. Yarger describes risk as inherent in all strategy and *"the best anyone can do to offer favourable balance against failure."*

The concept of strategy adopted by the corporate security unit drew on a combination of these. Strategy is best described as a "proactive, anticipatory and comprehensive risk based plan of action to address and manage unacceptable risk identified in phase one of the management model" (diagram 1). If it is accepted (as asserted earlier in this paper) that the risk and intelligence processes are complementary (if not the same process), then it can be said that intelligence was the driver of strategy within the corporate security unit.

Within the unit, management was aimed at achieving objectives through people, and strategy became the broader plan to achieve those objectives through changing behaviour (Maister, 1997). Policies became the resultant rules and guidelines that set limits for action and guided the behaviour of the personnel within the unit, and within the organisation (Mintzberg et al. 1991).

With intelligence considered as the driver of strategy within the corporate security unit, and with strategy focused on "ends" (achieving corporate objectives), then policy became the "means" to achieving those ends, through controlling unit and organisational employee behaviour. Policy, therefore can be said to have dominated strategy through an *"articulation of the end state and its guidance"* (Yarger, n.d.).

Hence policy could be considered a derivative of the same intelligence used to drive strategy within the unit (risk assessment). Intelligence was also used after implementation of the policy, to obtain feedback from stakeholders (executive, coal face staff, and internal/external audit), monitor whether it was actually achieving the objectives of the strategy or whether the policies (and indeed strategy) required change or amendment.

The ultimate value of intelligence is to guide policy makers in their decision making (Lowenthal 2006). In the model (diagram 1), risk assessment was used to provide the policymakers with information to best address the critical risks facing the business. That is not to say that the policy makers did not have input at the risk assessment stage. Strategic planning provided opportunity for policy makers to influence and shape the intelligence upon which their decisions were based. Ultimately it was that intelligence that provided the basis for decision making and ultimately supporting governance through, " doing the right things, in the right way, for the right people, in a timely inclusive, open, honest and accountable manner" (CIPFA, 2008).

5 Client relationships

Managing client relationships and ensuring client satisfaction is critical for any organisation or business unit. Rogers et al. (2007) described the client as the "beginning and the end", whilst Hartley (1994) observes that the ultimate test of an intelligence based product is client acceptance and whether any significant policy maker takes notice of the risk/intelligence assessment and changes policy. The value workshop model utilised at the corporate security unit had at its core a focus on the client. The unit also utilised elements of the internal consultancy model which focused on independence, security specialisation and upon delivery of expertise that can't be obtained by the client elsewhere.

The difficulty for the unit was often deciding exactly who its clients were and in prioritising service to them. Given the broad application of its services, the unit's client base varied to include company executives, shareholders, employees and customers, depending on the context of the service application. Corporate security and its associated intelligence products drew such a broad brush across both the strategic and tactical levels of the business that the unit often had to split its focus on delivery of services with resultant difficulties in resourcing and balancing competing interests of clients. Prioritisation occurred where risks were greatest, and this was normally based on criticality. Through communicative and consultative processes, the unit was able to build up an excellent strategic picture of the client's business, recognise and prioritise demands from competing and multiple clients, and manage the client's expectations.

Within the risk context, intelligence was heavily relied upon to provide a support function for critical asset protection. Major difficulties were often experienced through the client having unrealistic expectations of the time and effort involved in developing such intelligence, the difficulty in obtaining the necessary information, and the specialist skills required to support intelligence development (Ratcliffe, 2004). Client education, particularly at executive levels, communication and listening provided the solution to this problem by ensuring that the client and the unit had the same notion of task and desired outcome, particularly at strategy level. The corporate security unit first had to identify the multiple risk based services required by the client and then ensure that the programs developed met the expectations of the client, whilst at the same time ensuring that prioritisation was utilised to maximise the use of finite resources within the unit (Rogers, 1988).

Intelligence was utilised within the security unit as part of a systematic structured program of management, not only to obtain information regarding projects, tasks to be performed, skills required and time frames expected, but also to ascertain client preferences and priorities, challenge competing strategic goals, making sound strategic trade offs, tracking project time and costs, unit productivity and work quality (Maister 1997). Intelligence was also useful in assessing client satisfaction through feedback, thereby allowing the opportunity to improve service and build client relationships and confidence in the services provided by the unit. Intelligence facilitated ongoing direction, redirection and focus during projects and provided the mechanism for review and feedback post project. Ultimately, it provided a basis upon which to establish a *"security management institution"* where inclusive risk orientated considerations and arrangements became part of highly institutionalised managerial practice (Haftendorn, Keohane and Wallander, 1999)

6 Measuring performance

If two of the critical issues impacting upon client relationships are a focus or concern on the clients needs and how useful the intelligence was to the client and whether a significant decision maker used the intelligence to change policy, then the key to achieving these outcomes was feedback, continuous improvement and refinement of the intelligence processes to deliver progress towards achieving the corporate mission and objectives. This can only be achieved through measuring the performance of stakeholder groups within the organisation (Hartley, 1994).

Any management plan is incomplete without reliable and objective measurement criteria

to assess effectiveness, efficiency and quality of service. Rogers (1998) compares performance measurement with the nautical concept of taking sextant readings. Like its nautical cousin, performance measurement provides an indicator of whether the management program is on course. Within the management planning framework adopted by the corporate security unit (diagram 1), the compliance and investigation phases were used to measure performance and provide for continuous improvement. Compliance programs were used to ensure that the policy and strategy devised as a result of the risk assessments were being implemented, and that managers were *practicing what they were preaching*. Where control failures were detected, investigations were instigated to identify the cause and implement improvements.

Three major benefits arose from implementing effective performance management and measuring processes. The first was the unit's ability to evaluate its performance (in using intelligence) in assisting the development of strategy and policy to protect critical company infrastructure and assets. Next, it allowed the unit to monitor the activities of those charged with responsibility for implementing the strategies and policies, providing an early alert system to control failure and opportunity for remedial action. Finally, it allowed the corporate security unit and stakeholder managers to learn from experience to change or improve processes to enhance progress towards, and achievement of objectives.

There were a number of possible causes of control failure within the model. The strategy or policy may well have been based upon flawed intelligence (risk assessment) or alternatively, the failure might be due to non compliance of individual managers. Irrespective, these issues would be identified at the investigation phase and fed back into the risk assessment phase in a repeating circular process, thereby facilitating continuous improvement.

Intelligence played a critical role in the evaluation and measurement of performance by proactively providing insight into whether strategy and policy were working, and whether they were being effectively implemented by key stakeholders. It provided useful focus upon the areas most at risk and concentrated resources where they were most needed, thereby providing for accountability at both the stakeholder and security unit levels (Woodhouse, 1997).

7 Conclusion

Ultimately, the usefulness of intelligence in the context of strategic planning is in providing plans, oversight, guidance and direction. It links performance with the management processes. It enables managers of work units to make informed business decisions. It improves the timeliness and quality of those decisions, enhances communications with clients and stakeholders and measures satisfaction, thereby improving client experience. It ensures available information is directed and targeted towards achievements of objectives and identifies and addresses barriers and unacceptable risks to the business, thereby supporting corporate governance at multiple levels of the organisation.

The management planning frameworks adopted by the corporate security unit were the *Value Workshop* and *Consultancy* models, which drew heavily upon establishing client relationships and ensuring client satisfaction with the services provided. Within the context of the corporate security unit, risk assessment was critical not only in its context as a phase of the management model, but also in *identifying client's needs, wants and ultimately, satisfaction*. Policy and strategy were developed to address unacceptable risks and intelligence was then employed to not only ensure adequacy of, and compliance with policy and strategy, but to also measure progress towards objectives. The model demonstrated how risk assessment can be used to drive corporate strategy and ensure appropriate governance.

This paper looked at a management model implemented for a private sector corporate security unit (diagram 1). The intelligence function and risk assessment have been identified as essential elements of the model. The model has risk assessment at its core, a function that has been compared and overlaid with the intelligence process (diagram 2), to conclude that they are the same processes, supporting the notion of the convergence of intelligence and risk within a corporate context.

References

Apgar, D (2008) Increasing Risk Intelligence – How does your company manage risk? Retrieved 19/6/08 from http://www.businessweek.com/print/innovate/content/aug2006/id20060818_495984.htm

Australian and New Zealand Standard 4360:2000 - Risk Management

Bernstein, P.L. (1998) 'Against the Gods, the remarkable story of risk,' John Wiley and Sons. New York, pp 3 - 69.

Broder, J.F. (2000). Risk Analysis and the Security Survey, 2nd edition. Butterworth Heinman, Boston, p 139.

(CIPFA) Chartered Institute of Public Finance and Accountancy UK 2008, Improvement network. 'Governance, what is it about.' Retrieved 2/6/08 from http://www.improvementnetwork.gov.uk/imp/core/page.do?pageId=1007044

Christopher, S. (2004) A practitioner's perspective of UK strategic intelligence. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press, Australia, p 177.

Grieve, J. (2004) Developments in UK criminal intelligence, in Strategic Thinking. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press. Australia, p 25.

Hartley, J 1994, 'Concluding remarks', in Intelligence and Australia's National Security, A Bergin & R Hall (eds) Australian Defence Studies Centre, Canberra, pp 171-175.

Hewlett Packard (2007) 'Risk Intelligence Architecture – converting information to intelligence (White Paper), p3. Retrieved 15/5/08 from http://h20219.www2.hp.com/ERC/downloads/4AA1-5361ENW.pdf

Haftendorn, H. Keohane, R.O. & Wallander C.A. Imperfect Unions, Oxford University Press 1999, p 12.

Loves, M. (2000) *Fraud Intelligence Processing Systems* (Study Unit 8), Diploma in Fraud Management and Certificate in Fraud Control, Australian Centre for Security Research, University of Western Sydney, Macarthur, p 3.

Lowenthal, M.M. (2006) 'Intelligence, from secrets to policy, 3rd edn.' CQ press, Washington, p 9 - 174.

Maister, D.H., (1997). *Managing the professional service firm*. New York, Free Press, pp 179 – 224.

Mintzberg, H. & Quinn, J.B. (1991). The strategy concept, in *The strategy process: Concepts, contexts and cases*. 2nd Edn, Prentice Hall, Englewood Cliffs, NJ, pp 3-20.

Ratcliffe J.H. (2004) The Structure of strategic thinking. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press, Australia, pp 8 – 55.

Robbins, S, Bergman, R, Stagg, I & Coulter, M. (2006) 'What is management?' and 'What do managers do?', in Management, 4th edn, Prentice Hall, Sydney Australia, pp 4 -18.

Rogers K (1998), Evaluating strategic intelligence assessments: some sextant readings for law enforcement', Journal of the Australian Institute of Professional Intelligence Officers, vol.7. no.3. pp 23-94.

Rogers, K., Ure, J., & Young, L.J. (2007). *Intelligence Management*, Bathurst, Charles Sturt University. pp 3-11.

Stoner, J.A.F., Collins, R.R., & Yetton, P.W. (1985). Management in Australia, Sydney, Prentice-Hall, pp 16 – 128.

Woodhouse M 1997, Intelligence driven policing – A United Kingdom model' Journal of the Australian Institute of Professional Intelligence Officers, vol 6, no. 2, pp 49-111.

Yarger H.R. Towards a Theory of Strategy: Art Lykke and the Army War College Strategy Model. Retrieved 29/9/07 from http://dde.carlisle.army.mil/authors/stratpap.htm