Commercial intelligence?

Intelligence expert Martyn Denton, managing director at QRO Global, discusses the importance of evaluating risks and threats within the mining industry.

Issues of safety and security have always been a major concern for the mining industry. From the long standing threat of explosion and natural disaster, through to the more modern phenomenon of terrorism, companies involved in exploration and extraction are used to balancing a high level of risk with maximising returns and satisfying shareholders.

The industry is also currently experiencing some difficult times. As a capital intensive sector, rising costs and low margins have combined with a whole range of challenges, including the finance and management of capital projects, performance and operational improvement, sustainability, increasing resource nationalism – and amongst all these, the need to effectively manage risk.

Unstable environments

While mining companies have a history of venturing into new markets and regions, rising demand from countries such as China has resulted in many corporations looking further afield - often to riskier environments. In fact, Price Waterhouse Cooper's 2013 review of global trends in the mining industry predicts that further growth largely depends on activity in emerging and developing economies.

As a result, both surface and sub-surface organisations find themselves operating in an environment that offers exciting opportunities and rewards, but which is also accompanied by a significant element of risk. This makes good commercial intelligence, in its proper form, critical to success and ultimately, to safety.

Defining commercial intelligence

So, what do I mean when talking about the concept of intelligence as applied to commercial activity?

Traditionally associated with the military, intelligence has a vital role to play in identifying and developing global extraction markets, as well as driving business operations and answering the key questions that CEOs and shareholders are asking.

Often seen as primarily a security function with all the negative connotations that this inspires, successful intelligence is far more fundamental. In fact, mining companies should be placing the intelligence specialist at the heart of their operations to influence how business is done, to manage risk effectively and to ensure that board-level decisions on these operations are well-informed.

One of the first steps is to accurately define the terminology. The concepts of risk, threat and security are often misunderstood or poorly defined:

Security - in many organisations, the primary focus of any security department is to keep unwanted people out and to stop assets going walkabout. Some boardrooms view the security department as a necessary evil, often creating barriers and additional expense. Unfortunately, the function of security is often perceived as reactive when its real value lies in being proactive.

Threat - this is often used as a generic term by the security department to describe anyone or anything trying to breach their defences.

Risk - this is usually the main point of focus for the boardroom: What is the risk exposure? What are the costs involved? How is the risk going to change? In what order do we need to address the risks?

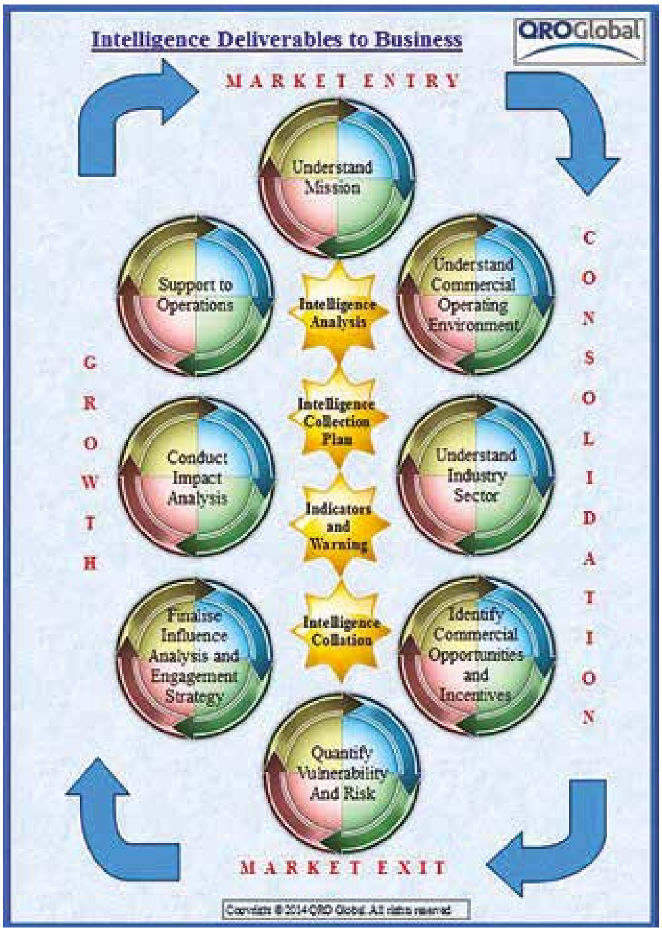
However, I would challenge these interpretations and advocate a more joined up approach to information management. For example, whilst identifying threats in an operating environment, it is likely that you would also be able to identify commercial incentives. Likewise, opportunities will become apparent during the risk assessment process.

A sense of understanding

The primary aim of intelligence work is to make sense of large quantities of uncertain, often conflicting, information that is collected and analysed for the purpose of achieving the company's objectives. The intelligence specialist should deliver a detailed insight into the operating environment, whilst presenting issues in perspective. Part of that process is managing organisational, cultural and personal biases and gearing the intelligence flow towards driving the decision-making process.

Questions that should be addressed and answered by intelligence specialists include:

- Which competitors are succeeding and why?
- How can we drive the business forward?
- Can we match the aspirations of the key decision makers?
- Where is the most advantageous operating environment?



- Can limited risk be managed to gain from opportunity?

We have already established that operating in the extraction industry has more than its fair share of risks. However, the flip side of this is the exciting potential within current and new locations.

Making headlines

Reputation is important whatever industry you operate in. Unfortunately, when things go wrong in mining, it often makes the headlines. Whilst tragic events are often perceived to be a result of security shortcomings, in reality they are more likely to be the result of a failure to fully understand the operating environment and its stakeholders.

Amenas, Algeria: The Islamist attack on the petroleum facility at In Amenas in Algeria which took place in January 2013 is a case in point. Operated jointly by the Algerian state oil company Sonatrach, BP and the Norwegian company Statoil, over 800 people were taken hostage at the site, 40 of whom died in the Algerian-led military rescue assault. The Statoil report on the incident contains some significant observations on security and the role it played in the tragedy.

The report concluded that “security is not established as a corporate function independent of safety, recognised for its distinct characteristics and requirements. In most cases security is a small part of broader health, safety and environment positions, and one for which few people in those roles have particular experience and expertise.”

Statoil’s management was criticised for failing to place security and intelligence at the heart of its operations, with the report recommending that Statoil strive to develop a “strong and coherent security culture in the company…. it must be an intrinsic and embedded part of the company’s core activities.”

The report recommended that the company “improve its ability to detect, delay and stop potential attacks by reinforcing electronic and physical protective measures, enhancing its security risk management capability and developing a coherent programme of security training and exercising, whilst broadening and deepening co-operation with relevant government agencies and organisations.”

While the report offers some important lessons that the whole industry can learn from, it’s unclear whether it fully acknowledges the need for a wider perspective and knowledge of the situation. In fact, there is an underlying sense of building the fences higher and reinforcing the physical barriers when what is needed is the implementation of systems to help predict the likelihood of such an attack arising again.

Somair, Niger: In May 2013, al-Qaida-linked suicide bombers attacked the French owned Somair uranium mine in northern Niger killing one member of staff and wounding 14 others. This was in reaction to the French-led military intervention in Mali in January that year.

With France heavily nuclear-dependent (nuclear reactors produce 75% of the country’s electricity), the impact of such attacks has significant implications for both Niger’s economy and the French nuclear industry. The attack not only had a cost in terms of human life, but also meant that the site was not fully operational for three months at an estimated cost of US$35 million a month.

Worryingly, security at the Somair mine, which is supplied by Niger forces, had already been reinforced twice after other attacks. This raises serious questions about future security at the site, and the success of the company’s policy of on the ground operation and integration.

To function profitably and safely within an unstable environment, an organisation must accept that this involves far more than the granting of a licence to operate by the relevant government. The process involves engaging with a whole range of stakeholders, from the government to local communities.

Spending ever increasing amounts of money on security will almost certainly fail if local and regional problems aren’t addressed and used to inform practice.

The role of intelligence in market entry

I have been recently involved in a market entry and consolidation project in a developing African country which has benefitted hugely from the input of intelligence.

This example deals with an exploration project in an isolated area of Africa where a disastrous event could occur in the future if the right action isn’t taken at the outset.

The region has a limited infrastructure and high levels of crime and poverty, but offers potentially lucrative returns for the right commercial intervention. The company’s security specialists advise that everything is currently satisfactory as there is a strong military presence in the area and crime has been reduced in recent years.

The military is friendly and co-operative and the security specialists assert their confidence in the military’s capability and intent. The board is using these assumptions as the basis for its decision-making.

However, the situation really merits closer inspection as there are real problems with this line of thought, and many important questions to be asked:

- Do they fully understand the factors that could influence the openness of the military?
- Do the military really understand what is happening in such an isolated area?
- Can the military be relied on to always be located there

in their current strength?
- Are the military being completely open as to the causes and effects in crime levels?
- Are the company aware of the methods employed by the military in maintaining control?

In short, is the military unbiased in this situation? On current evidence, the answer to all of these questions appears to be no.

Furthermore, a cursory glance at the wider situation reveals other significant factors. The political system is centralised, unstable and one in which no commercial organisation would want to be involved should there be sudden regime change.

It is likely that the commencement of operations by a Western company would dramatically change the societal dynamics of the region, whilst the influence of other foreign companies who may have less ethical business and environmental practices needs to be considered.

Ominously, this scenario contains some similarities to In Amenas and the Somair mine, i.e. security being driven by personnel on the ground who are dealing with the hard realities of implementing physical security measures on site. Using military terminology, these people are viewing the situation through the sights of a gun, giving them a very limited perspective.

The intelligence process – implementing the six Cs

Many of the markets that mining companies operate in are high risk due to a wide range of factors from political instability through to terrorism and natural disaster - to name but a few. To succeed in these difficult and unpredictable environments, companies need a proactive intelligence-led approach to business operations.

The diagram represents what an intelligence expert should be able to deliver to a board of directors in order to support market entry, market exit and growth or consolidation of their business interests. The eight outputs are underpinned by four key intelligence functions in the centre.

Intelligence-led business operations can be broken down into the six Cs: concept, context, challenges, chances, choices and conduct.

Concept: the first stage is creating a business objective that is well-defined and understood at the concept phase. This is key to providing a common direction.

Context: this is the core of the intelligence work and centres on the principles of intelligence to effect a collection plan and to then transform the resulting information into actionable quantified intelligence. The intelligence picture is broken down for ease of application into:
- Basic - what happened yesterday?
- Current - what is happening today?
- Applied intelligence - what will happen tomorrow?

In business, the decision-making process is often supported only by basic intelligence with limited current or predictive analysis. Such 'basic' information can be readily bought from various sources in so-called 'risk assessments' for particular countries or environments.

Although of some use, they need to be recognised for what they are: a rudimentary start to the process. Intelligence specialists are able to deliver a much greater understanding, including a detailed appreciation of the incentives and disincentives present in the operating environment.

Challenges: a detailed assessment is made of the identified disincentives in context with the vulnerabilities of an organisation as seen in relation to achieving the objective. The result of this work is the risk matrix; a prioritised list of risks to the achievement of the objective, the impact on the business and recommendations to mitigate the risks.

Woven into this risk matrix are potential courses of action by adversaries and other operational players, as well as the indicators and warning - a red flag system to prompt action in response to a changing operating environment.

Chances: at this stage, a developed understanding of the situation allows for an assessment of business opportunities for the particular industry sector.

Choices: this is the planning phase, when all the previous intelligence work is used to define the relationship that exists between people and organisations in the operating environment, the mission and an organisation. These relationships are captured in the Influence Analysis and serve to drive the thought process for determining actions, as part of the Engagement Plan, shaping the operating environment. An analysis of the impact pulls all negative and positive consequences together before the final decision is taken to implement the plan.

Conduct: finally, real-time intelligence support to business operations is given during the execution phase.

This process ensures that executive decisions are based on a realistic and detailed understanding of the operating environment. It provides a set of quantified future opportunities and risks, backed by evaluated solutions, approaches and responses.

Key questions such as 'So what?' and 'What now?' help to ensure that the process is appropriately forward looking.

Events across the world regularly prove that underestimating or misinterpreting the environment in which you operate or plan to set up can have disastrous results. Inevitably, if the returns are suitably lucrative, companies will continue to operate in areas of significant risk, putting in more security safeguards and paying increased insurance premiums in an attempt to prevent further events.

However, reputations, profits and even lives can be saved if mining companies make effective use of intelligence to ensure that any forays into new markets and opportunities are based on the understanding necessary to balance risk and reward.

About the author

Martyn Denton is MD of QRO Global who offer a range of intelligence services to business. Martyn has over 30 years' experience in the armed forces, reaching a senior level within the British Army. Martyn has been involved in intelligence operations across the world in both a military and commercial capacity, working in co-operation with the armed forces, law enforcement agencies and government departments of both the UK and foreign nations.

www.qro-global.co.uk