The Financial Aspects of the Security of Assets and Infrastructure in the Energy Sector

A Set of Guidelines Prepared by the Harnser Group for the European Commission

Autumn 2012

Contract No: ENER/B1/ETU/42-2011/SI2.611505

Contents

Foreword

Any risk has a financial consequence and security risk is no different.

These Guidelines are aimed at the owners and operators of energy infrastructure Assets across the EU to raise awareness about the financial consequences of managing the security risks to those Assets.

It is hoped that the Guidelines will not only be of interest to energy companies themselves, but also to other stakeholders who have an interest in the risk and financial management of energy companies and the shareholder value they create.

The European Union (EU) is developing its policy on the subject of the security of Critical Infrastructures in relation to its strategy on the security of supply. The energy supply system, vital for the well being of the citizens and the functioning of the economy, is considered as a priority for the establishing of European measures oriented to improve, where necessary, the level of protection of its critical infrastructures. One major step in this policy was the adoption of the European Programme for Critical Infrastructure Protection (EPCIP), a cornerstone of which is the Directive 2008/114/EC, on the Identification and Designation of European Critical Infrastructure (ECI) and the Assessment of the Need to Improve their Protection. Further details on EPCIP are set out in Box 1.

In the context of EPCIP, the European Commission (EC) acknowledge that a good understanding of the true financial cost of managing the security risk to energy facilities and infrastructures in the EU would be beneficial to their owners and operators, as well as those who are engaged in developing policy pertinent to the Internal Energy Market. Tender No. ENER/B1/2011-42 was commissioned by the Critical Infrastructure Protection division in the Directorate-General for Energy, responsible for the implementation of the EPCIP programme for the sector, and the work to prepare a set of Guidelines for the energy sector was awarded to Harnser Risk Group.

Box 1.

In December 2008, as one of the elements of EPCIP, Council Directive 2008/114/EC 2 on "the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection" was formally adopted by the Council. The Directive was accompanied by guidelines for implementation (containing the sectoral and cross-cutting criteria needed to identify European Critical Infrastructure "ECI") which were also endorsed by the Council. The Directive constitutes a first step in the identification and designation of ECIs and assesses the need to improve their protection. As such, it concentrates initially on the energy and transport sectors.

The basic obligations of the Directive include:

- Each Member State takes forward and participates in the identification and designation of relevant ECI;
- Owners/operators of designated ECI must implement an Operator Security Plan (or equivalent) and designate a Security Liaison Officer;
- Member States perform threat assessments concerning specific sub-sectors in which ECI have been identified on their territory;
- Member States report to the Commission on the types of threats, vulnerabilities and risks identified in each sub-sector in which ECI have been identified on their territory;
- Each Member State designates a formal ECI Protection Contact Point;
- Based on the information gathered through the ECI process, the Commission and Member States shall assess whether further protection measures should be considered for ECIs.

Acknowledgements

Writing a set of Guidelines requires a team with the experience and ability to look at the risk from different perspectives.

To achieve this, we sought the advice of experienced security risk practitioners and their colleagues in a number of energy companies to complement the views of our own team.

We also consulted the views of of Fitch Ratings and, in particular, Mr Erwin van Lumich, Managing Director, Head of EMEA Energy, Utilities & Regulation; and Mr Raj Singh, former Member of the Executive Committee and Board and Chief Risk Officer of Swiss Re. Mr Singh was also a former Chief Risk Officer at Allianz SE, founding Chairman of the 'CRO Forum', the association of Chief Risk Officers of the top 20 insurance groups and; former Chairman of the International Financial Risk Institute.

Their input has added immeasurably to the Guidelines and our thanks go to all of them.

Chapter 1
Introduction

1 Introduction

Security risk has an impact across most of the corporate value chain. It is a natural consequence of the economic activity undertaken by an energy company to deliver the strategy agreed by a Board of Directors to create shareholder value.

Like any other risk, it also has a financial consequence, as shown below in Fig. 1.1, and the Guidelines are intended to answer the question: 'What is it'?

This Introduction explains what security risk is, what it means in the context of energy infrastructure and Critical National Infrastructure (CNI), how security risk is perceived and managed within energy companies. Each of these factors drive the financial aspects of securing assets and infrastructure.

Fig. 1.1 Impact of Risk Events on Financial Performance

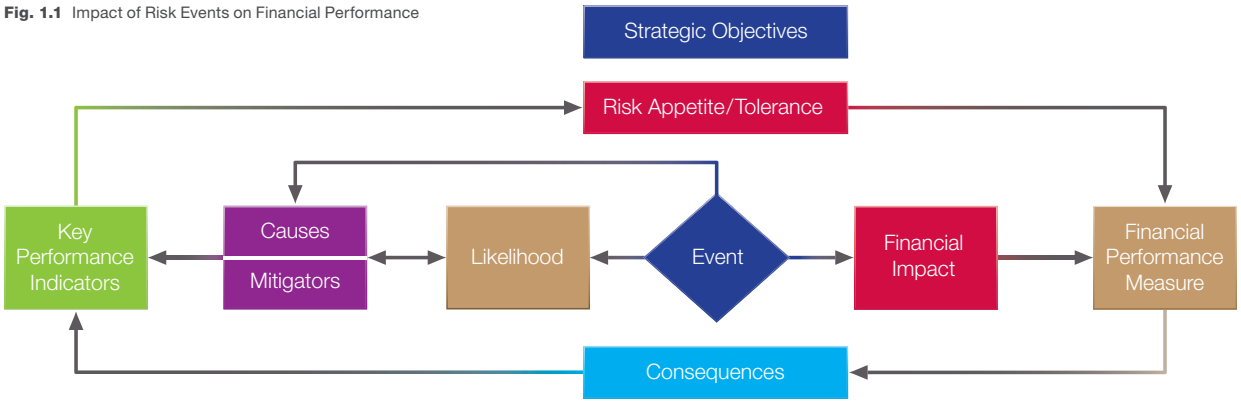


Fig. 1.1 Notes of explanation

(1) To achieve Strategic Objectives an energy company accepts an agreed level of risk tolerance – this must be confirmed.

(2) An Event is a scenario that results in a variance from those objectives – these must be identified.

(3) The event can be caused by a single, or multiple action(s), or inaction(s), which can be mitigated by either good preventive measures or post-event management activity. Causes can be identified and mitigators agreed.

(4) The Likelihood of the event occurring can be modelled for all security risks. By multiplying likelihood and impact an index is created for ranking purposes and to aid prioritisation.

(5) The Financial Impact of an event can be known and should be identified.

(6) Assess the financial impact on pre-determined Financial Performance Measures relating to the Group and business units.

(7) Consequences over and above the financial impact can be identified and reviewed.

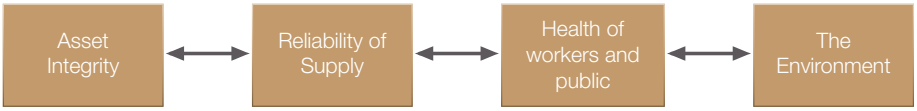
(8) Create Key Performance Indicators which could act as early warning indicators and causes and events. An energy company can then monitor and identify performance trends against accepted tolerance levels.

1.1 Definitions of Security Risk

There are a number of definitions of security risk. One by Julian Talbot and Miles Jakeman refers to a security risk as "any event that could result in the compromise of organizational assets. The unauthorized use, loss, damage, disclosure or modification of organizational assets for the profit, personal or political interests of individuals, groups or other entities constitutes a compromise of the asset, and includes the risk of harm to people. Compromise of organizational assets may adversely affect the enterprise, its business units and their clients. As such, consideration of security risk is a vital component of risk management". [1]

The one used by the European Commission refers to the Oxford English Dictionary definition of security as **"the safety of a state or organisation against criminal activity such as terrorism or espionage".**

For **energy infrastructure**, the **goal of security** is to take *prevention, mitigation and responsive measures* across the supply chain to ensure the following:



In doing so, security risk is similar to how other risks are evaluated insofar as it looks at an Asset (facility, structure, etc.), potential threats, probability (likelihood and vulnerability), severity and consequences.

Like any other risk, **security risk**:

- Requires specialist knowledge and experience [2]
- Needs to be managed within a defined risk governance framework
- Needs support from within an organisation; and
- The endorsement of the Board of Directors as the ultimate 'owners' of the risk.

However, **security risk is also unique**, most notably because of the highly confidential nature of the risk itself. Security issues are often matters of national security interest with the involvement of security services, police and government authorities.

So it is not possible to undertake the kind of probabilistic modelling that can be undertaken on other risks where data records of incidents and impacts are more readily available, for example, in relation to natural hazards such as flooding, earthquakes etc. **However, this does not mean diminish the importance of undertaking rigorous analysis, rather it underlines the necessity of doing so.**

1.2 Critical National Infrastructure (CNI)

The security and economy of any country and the well-being of its citizens depends on certain infrastructure and the services they provide. This is known as **Critical National Infrastructure** (CNI), the destruction or disruption of which could result in the loss of lives, the loss of property, a collapse of public confidence and moral in government and financial institutions. Any potential disruption or manipulation of CNI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of countries, their citizens and the EU.

There is a high degree of interdependency between CNI sectors at a local, national, regional and global level, as shown in Fig 1.2. The resilience of CNI is a multi-layered issue that draws together the interests of trans-national organisations such as the EC and NATO as well as governments, who have a role to play in identifying inter-dependencies and impacts across their own CNI, or European designated Critical Infrastructures.

Under a CNI strategy, CNI Asset Owners should understand what role they play in ensuring resilience as well as the support available to them from the host or home government.

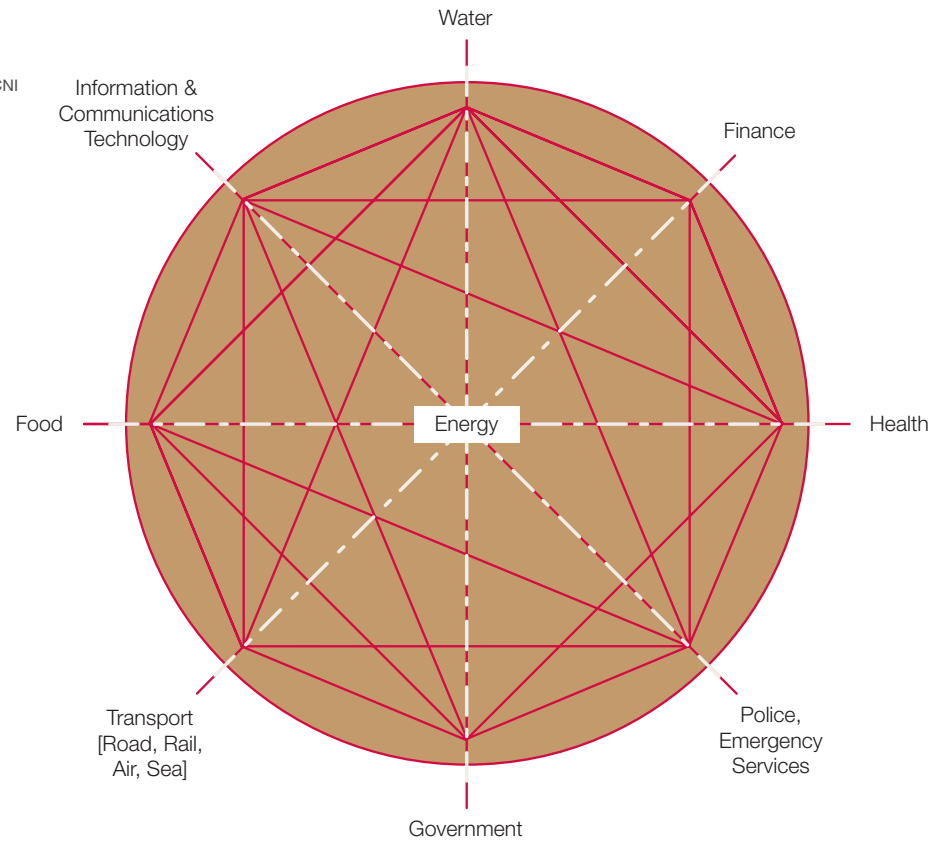


Fig. 1.2 Inter-dependencies between CNI

EPCIP reflects the EC's evolving policy in this area and one glance at a map of European oil and gas pipelines and networks demonstrates that a purely national approach to CNI is no longer viable. **Instead, a joined-up approach across the supply chain to ensuring the security of supply is necessary**, one that minimizes the risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory. Also that additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimized, or transporting across more than one Member State. These are issues relevant to discussions about the Internal Energy Market [IEM].

1.3 Resilience

Resilience has become a topical issue not only in the context of CNI, but across all companies and organisations who face potential disruption from risks.

Many governments are developing their strategies in relation to the resilience of CNI Assets. Governments have a particular role in identifying inter-dependencies and impacts which are crucial to the planning required to deal with an event or incident that disrupts different sectors. As noted in Fig. 1.3, managing resilience requires **all parts of what might be described as "a Resilience Chain" to work together.**

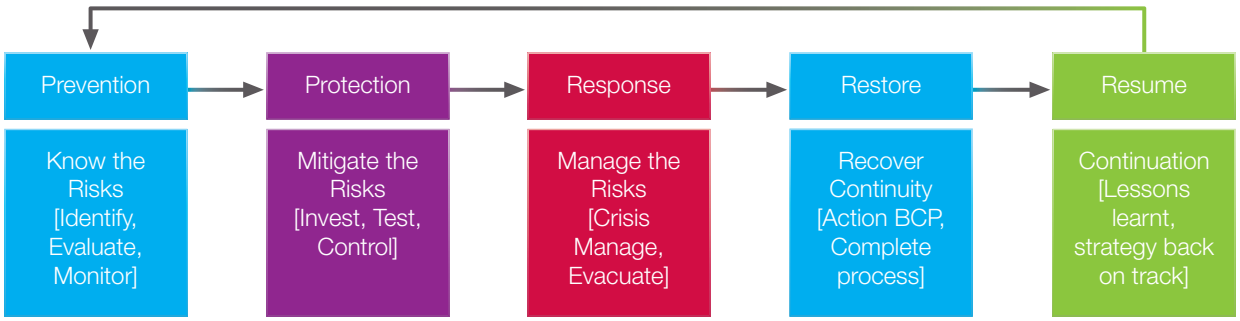
---

[1] *Julian Talbot and Miles Jakeman "Security Risk Management Body of Knowledge" John Wiley & Sons, 2009.*

[2] *Specialist knowledge is crucial, as it would be with Credit or Market risk, but that does not mean that the risk cannot be managed using a similar governance structure.*

[3] *There are a number of sectors that include assets classified as part of the CNI for example, water, health, finance, however, the energy sector is usually the largest of all CNI sectors and the most important.*

Fig. 1.3 A 'Resilience Chain'



Given the consequences and financial impact that can occur [see 1.4 and Chapter 4] from a risk event, it is clear that **ALL parts of the Resilience chain are critical to an organisation**. However, in some quarters, the debate about 'resilience' is dominated by a focus on Response, Restore and Resume. Certainly work on Crisis Management and Business Continuity Planning has evolved to the point where there are emerging 'standards' which, in the energy sector, have also been driven by HSE requirements.

In some instances less attention is focused on 'Prevention' and 'Protection'. One reason is that there is just more experience of dealing with natural hazards and safety incidents, where probability and impact is known and can be modelled with greater certainty, than is possible when dealing with criminal, and especially terrorism, threats. This is not only because of national security concerns and the sensitive nature of the risk, but also because of how security risk is perceived and managed with organizations. This is noted more in 1.5.

EPCIP itself focuses on the impact of the disruption from a risk event and as such takes an all-hazards approach. **However, the EC acknowledges that when considering protection measures the nature of the threat and the vulnerability has to be considered in more detail; and with a greater experience of dealing with natural hazards and component failure, protection measures need to focus more on criminal and terrorist threats.**

The Guidelines are designed to help an energy company identify the costs of ensuring resilience through risk identification and planning. Getting the balance right between each part of the 'chain' is important so that a Board of Directors has the assurance that with the right preventive and protective measures in place, the likelihood of the organization needing to respond, restore and resume is as low as reasonably possible given the risk appetite of the Board.

It is important to note that the Guidelines do not cover the loss of earnings, competitive positioning, impact on reputation and share price that can arise as a consequence of a security event occurring, but these can be significant and need to be taken account of in the development of the Security Strategy.

1.4 Energy Infrastructures

Energy is the largest CNI sector in any country supporting all other sectors.

Energy infrastructures represent unique targets for a variety of reasons, including:

- Their central importance within national and regional CNI networks.
- Their political and strategic importance.
- The potential for immediate impact – mass damage and casualties.
- The potential for consequential impact – further casualties, contamination, loss of service delivery.
- Multiple targets, often at single locations – personnel, Process Control/SCADA systems, hazardous materials and general infrastructure such as buildings.
- Multiple inter-dependencies across the supply chain.

The threat groups that could conduct attacks against energy infrastructure are set out in Table 1.4.1 along with the potential financial impact. Within these threat groups are a range of sub-categories which demonstrate the breadth of interests, whether driven by religious extremism or environmental activism carried out by single issue groups or retribution by a disgruntled employee.

Table 1.4.2 shown as an Annex to this Chapter summarises the nature of these threats along with wider consequences. [See Chapter 4 on Understanding the Financial Impact of Security Risk].

Table 1.4.1
Financial Impacts of Threats

Threat Type	Sub-Category	Financial Impact
Terrorism	International Terrorism Individual 'Lone Wolf'	• Damage to assets – repair and replacement costs • Cost of outage time • Reputational damage • Increased cost of financing • Increased insurance costs • Loss of staff – replacement and training costs • Staff retention problems • Staff recruitment problems • Supply chain disruption leading to operational outage • Increasingly difficult operating environment • Compensation costs • Lawsuit costs • Bribery costs • Corruption costs • Fraud costs • Loss of competitive advantage • Loss of contracts • Loss of customers • Compliance costs • Nationalisation • Loss of sensitive information/assets/material • Increased security costs – physical, technical, procedural, personnel
Criminal Activity	Workforce and/or Disgruntled employees Contractors and/or Visitors Sophisticated Criminals Opportunistic Criminals and Vandals Deranged Individuals	
Subversives	Foreign Intelligence Services Competitors Hackers	
Civil Unrest	Violent political change Domestic Activist Groups	
Cyber Crime	Penetration Attack Introduction of Malware Denial of Service Attack	
Natural Hazards	Drought Flash Flood Sandstorms	
Accidental Hazards	Fire and/or Explosion Containment Failure	
Consequential Hazards	Production Outage Loss of Suppliers Loss of Transport Loss of Employees Proximity Hazards	

It is worth noting here that target attractiveness has a significant influence on the likelihood of an attack against energy infrastructure and assets.

By way of example:

- Is the threat present?
- Does the threat have an inherent capability to achieve its objectives – for example means of access, level of professionalism and use of weapons and method of delivery?
- Does the threat have the intention to act?
- Has the threat targeted this facility/sector/country region before?
- Are threat sources likely to recognise the potential value of the target?
- Do these characteristics offer the potential to fulfil the adversary's core objectives?
- Does the balance between risk and reward lie in their favour?
- Is this the best option for them or can their objectives be achieved more cost-effectively elsewhere?

Given what was noted earlier about the focus on Prevention and Protection, it is important to understand the nature of the threats posed to energy infrastructures and assets, the likelihood of a potential attack and its severity. Then appropriate risk mitigation strategies can be put in place to reduce the risk to what the Asset Owner regards as acceptable, including responding to that risk IF it occurs.

Without this link, cost overruns are inevitable.

Table 1.4.2
Threats to Energy Sector - Possible Attack Characteristics and Consequences
(Source RSMP & PRISM®)

	Attack Characteristics		
Threat Scenario	**Planning & Professionalism**	**Possible Means of Access**	**Use of Weapons**
Terrorist Scenarios			
Multiple near simultaneous VBIED/IED attack on facility & personnel	Determined attack, extensive training, recruitment and/ or radicalisation, hostile reconnaissance and practice run/ test of security	1. Penetrative vehicle attack through perimeter 2. Parked in adjacent area 3. Bypass vehicle access controls	Fuel tankers, vehicles, IEDs, possibly firearms, possibly chemicals (i.e. Chlorine enhancement)
Hand-placed IED attack on Critical Components	Training, recruitment, hostile reconnaissance and practice run/ test of security	1. Forced entry with manual/ specialist tools 2. Bypass of access controls 3. False Credentials 4. Insider Collusion/Social Engineering	IEDs, firearms, improvised or specialist intrusion tools
Close Quarter Attack on facility personnel	Determined attack, extensive training, recruitment and/ or radicalisation, hostile reconnaissance and practice run/ test of security	1. Overwhelm Guardforce 2. Possible use of vehicles or boats to access target	Firearms, grenades, blades, possibly IEDS
Stand-off RPG/Mortar attack on facility	Training, recruitment, hostile reconnaissance	No access required	RPG, Mortar, Firearms
Sabotage of Plant causing deliberate off-site release of hazardous materials	Research into facility processes	1. Forced entry with manual/ specialist tools 2. Bypass of access controls 3. False credentials 4. Insider access	Blunt objects, possibly blades, firearms or explosives. Improvised or specialist intrusion tools
CBR contamination of water supply or building	Extensive planning/training/ resources. Possible hostile reconnaissance and dry run	1. Forced entry with manual/ specialist tools 2. Bypass of access controls. 3. False credentials 4. Insider access	CBR materials, improvised or specialist intrusion tools, weapons
Kidnap of senior executive(s) for political or financial reward	Planning and hostile reconnaissance to identify movements.	1. Overwhelm Guardforce 2. Utilise movements in public areas	Blades, Firearms and possibly explosives
Maritime vessel used as Water-borne IED/Light aircraft used as Airborne IED	Determined attack, extensive training, recruitment and/ or radicalisation, hostile reconnaissance and practice run/ test of security	1. Penetrative attack 2. Target co-located hazardous facility for domino effect	Aircraft/Vessel, IEDs, firearms
Criminal/Subversive/Activist Scenarios			
Cyber attack on SCADA system resulting in loss of control over critical plant processes.	Experience and perhaps specific training. Not necessarily determined since can be carried out remotely. Possibly state-level resources.	Social engineering, insider access/ collusion, remote access, physical access to SCADA system.	Electronic devices (USB sticks, CDs, wireless receivers etc), malicious software/scripts.
Theft of highly sensitive corporate data.	Planning, hostile reconnaissance and dry run	Insider access, physical intrusion, hacking	Physical attack tools, electronic hardware and software
Physical sabotage of plant by disgruntled employee	Possible planning but could be instinctive	1. Forced entry with manual/ specialist tools. 2. Bypass of access controls. 3. False credentials 4. Insider access	Blunt objects, improvised intrusion tools
Protestor/activist intrusion at multiple sites – deliberate release of product and forced shutdown of plant.	Moderate determination, planning and training. Possibly hostile reconnaissance and testing of security measures	1. Forced entry with manual/ specialist tools. 2. Bypass of access controls. 3. False credentials 4. Insider access	Hand-cuffs, chains and padlocks, improvised and specialist tools
Loss of supply from external dependency.	Supply interruption at very short notice and without any prior indications		
Large-scale attack on an adjacent infrastructure with domino impact on facility.	No prior notice although obvious high-risk facility posing potential off-site hazard		

	Worst-case Consequences		
Method of Delivery / Initiation	**Assets at Risk**	**Primary Consequences**	**Secondary Consequences**
Vehicle Borne & Person Borne, suicide, remote detonation, timer, tripwire	Entire facility – plant and people	Catastrophic damage to facility, long-term production outage, loss of containment, extensive loss of life. Domino effect on adjacent infrastructure	Damage to wider economy, loss of public/employee confidence, litigation, reputational damage, impact on share price.
Timer, remote detonation	Critical Points such as transformers, valves, storage tanks	Long-term production outage/ loss of revenue, possible loss of containment or life	Loss of confidence by customers, contractual penalties, damage to reputation.
Moving shooter attack and/or sniper/protected positions. Possibly kidnap to discourage interdiction by response force	Employees, contractors and visitors	Extensive loss of life	Litigation, reputational damage, loss of confidence by employees, share price
Stand-off from remote 'base-plate'. Capability to fire over obstructions	Critical Points or facility as a whole, particularly if domino effect	Loss of production/revenue/ life. Domino effect on adjacent infrastructure	Litigation, reputational damage, loss of confidence by employees, share price
Intrusion, manual attack on plant or interference with physical controls	On-site staff, local populations, co-located facilities, environment	Widespread casualties, short and long-term health impacts, environmental damage, short-medium term loss of facility for clean-up	Litigation, change in regulatory environment or loss of operating license, damage to economy/ reputation/share price
Intrusion and introduction of contaminant. Use of HVAC system or water storage tanks. Access to off-site supply route	People and facilities (facility may have to be destroyed if cannot be decontaminated	On-site casualties and possible off-site spread if not detected early	Public fear, loss of confidence by employees, reputational impact, drop in share price
Use of force to overcome any Close Protection. Taking when at home or in transit	Senior executives and families	Financial loss, impact on operational capability, forced into political/public statements that could damage company	Reputational damage and impact on share price
Penetrative suicide attack or remote detonation	Facility as a whole and personnel	Catastrophic damage to facility, long-term production outage, loss of containment, extensive loss of life. Domino effect on adjacent infrastructure	Damage to wider economy, loss of public/employee confidence, litigation, reputational damage, impact on share price
Over network or via connection of physical device.	Critical functions and processes.	Loss of Containment/Production Revenue. Potential off-site release, explosion or long-term damage to plant	Loss in public/govt. confidence, change in regulatory environment, loss of reputation/share price
Covert entry and escape	Hard and soft copy data	Loss of competitive advantage, contracts, revenue	Extensive damage to market share, reputation. Possible litigation
Intrusion, manual attack on plant or interference with physical controls	All plant infrastructure	Financial loss through damage to plant, loss of containment/ production revenue especially if domino effect, possible loss of life	Supply-chain impacts, loss of reputation, contract penalties etc
Mass protests, intrusion, lock-on's, manual interference with plant - attempt to force shutdown	Plant infrastructure vulnerable to manual interference and/or damage	Loss of containment/production outage/loss of revenue. Possible casualties amongst protestors	Litigation for duty of care to protestors, environmental damage and clean-up costs, impact on reputation and share price
	Production	Forced shutdown/loss of production	Contractual penalties, impact on share price
	Plant, shared utilities/access routes/infrastructure.	Loss of shared infrastructure/ utilities/access routes, some explosion damage, requirement to evacuate facility for x days/weeks and therefore loss of production	Impact on resources, market confidence, share price, contractual penalties

1.5 The Profile of Security Risk

The level of interest in security risk has risen over the last few decades and is expected to increase. The nature and extent of security threats is growing and changing with consequences that extend beyond the primary target. The conclusions from the 2011 Global Risk Report, published by the World Economic Forum, focus on Economic Disparity and Global Governance Failures as two key drivers of the global risk environment, reflecting changes that governments and companies have little influence over. Many of those changes raise security concerns and are ongoing drivers.

However, there is a "**two-speed debate**" in many European countries, if not all, between those with an interest in the security of supply and the protection of CNI Assets, and the Asset Owners who often have to pay for that protection. A consensus is required between those with a national or regional responsibility for the security of supply and protection of CNI assets, and those who own the Assets and are accountable to shareholders for the financial choices they make.

This will become more important as pressures converge on all parties from geo-politics, technology, demands for energy, corporate accountability and transparency, public expectations about governance and duty of care etc.

Aligning interests and delivering a joined-up approach which reflects the dynamic and cross-border nature of energy markets is still a long way off and there are several challenges to overcome before that can happen. These also hamper the ability of an energy company to identify the true cost of managing its security risks.

These challenges are:

1.5.1 Low perceived added value

Security risk tends to be managed differently from other risks such as Health, Safety & Environmental (HSE) or operational risk which business owners tend to be more involved with and have greater flexibility and control over. HSE in the energy sector has evolved into a well regulated and standardised approach. Whilst security is often incorporated within the HSE department, it is a very different risk and can be marginalised alongside the more familiar, well funded and regulated HSE risk.

As a result, the business owner can be less engaged and often has less knowledge of the subject than other risks. Security risk is not regarded as a business enabler and is often disconnected from the strategic analysis and planning processes.

The Guidelines will show how security risk needs to be aligned alongside strategy and subject to the same review as other risks that influence the growth potential of the business.

1.5.2 Corporate Competency

Most energy companies rely on the experience of a relatively small number of individuals to look after the security of all sites and facilities. This experience is critical, but it would be rare for a company to say it had a corporate competency or capability in security risk management – a statement it would certainly make about HSE risk.

This means that the **approach** taken towards the identification, assessment and mitigation of security risk can vary across the business, as well as the sector – and this does have financial implications.

1.5.3 Methodology

Unlike HSE, there are no internationally recognised standards about how to manage security risk. There are a number of well regarded risk assessment guidelines in the sector, but these only cover part of what is required. At the core of any security management approach there is a good risk assessment process, but that needs to be based on an understanding of strategy and risk tolerance set by the Board of Directors and it must be linked to specific performance-led design principles, reporting and monitoring. Concepts similar to Enterprise Risk Management (ERM) (see Box 1.1).

1.5 The Profile of Security Risk Cont.

1.5.3 **Methodology** cont.

Box 1.1.

Defined by the US 'Committee Of Sponsoring Organizations Of Treadway Commission' (COSO) as, "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." COSO divides ERM process into eight components: (1) internal environment, (2) objective setting, (3) event identification, (4) risk assessment, (5) risk response, (6) control activities, (7) information and communication, and (8) monitoring.

A different risk assessment process across different sites in a large energy company leads to a different set of protection objectives and risk mitigation measures.

From a financial perspective, this has several implications:

- If security measures are viewed as fragmented or ad hoc, it is difficult to argue against requests to reduce costs around a site or facility. Explaining the impact on vulnerability and inter-dependencies is difficult without a broader analysis of what the risks are. **Given the challenge posed by low perceived added value, inevitably any company will try to minimise what they spend on security risk, unless told otherwise.**
- Without a common methodology and defined risk-based performance standards, **economies of scale are harder to achieve in the purchase of equipment, expertise and insurance**.

The RSMP was published by the European Commission in 2010 to aid the preparation of a Security Management Plan for owners and operators of energy infrastructure assets. It is based on the PRISM® process which introduces ERM principles and concepts to security risk to address the challenges noted in this Chapter.

1.5.4 **Risk Pricing**

Without a common methodology it also becomes difficult to price the security risk. If a company knows the cost of its aggregate security risk, it will try to offset that cost either into the cost of operations, or through insurance, or through the price of the end product, something in many countries that is regulated and may not be permissible. So the cost of the risk has to be borne somewhere.

The question of pricing for risk also becomes relevant in the context of the Internal Energy Market (IEM). Looking ahead to the EU's aspirations for the IEM (see Box 1.2) the need for a level playing field becomes apparent, although this will not be without its challenges simply because of the differentials between regulation, the pricing of risk and the ability to offset the cost of regulation for the companies involved.

Box 1.2.

"The existence of a competitive IEM is a strategic instrument in terms of both giving European consumers a choice between different companies supplying gas and electricity at reasonable prices, and of making the market accessible for all suppliers, especially the smallest and those investing in renewable forms of energy. There is also the issue of setting up a framework within which the mechanism for CO^2 emission trading can function properly. Making the IEM a reality will depend above all on having a reliable and coherent energy network in Europe and therefore on infrastructure investment. A truly integrated market will contribute to diversification and thus to security of supply."

The European Commission

1.5 The Profile of Security Risk Cont.

1.5.4 Risk Pricing

This point is explained in more detail below:

- As security risk management always has a financial consequence to it, if countries within the EU set security standards for European Critical Infrastructures (ECI) Assets or indeed if some EU countries require all CNI Asset owners to adhere to different security standards – **not only does this create a vulnerability and risk transference within a sub-sector**, it also **creates a cost arbitrage**. This is not new and has occurred for many years in the financial sector where the cost of regulation has shaped innovation and pricing. There needs to be consistency throughout the supply chain, and this may require regulation for the reasons cited earlier.
- The reference made to the existence, and planned elimination, of **energy 'islands'** by 2015 underline the importance of smoothing discrepancies between how individual EU markets operate at present. Energy supply is a matter of national security interest and encouraging liberalisation will therefore be a challenge. Assurances will need to be made about competition and monopolies addressed.
- Where the IEM involves energy companies who are incorporated **outside the EU**, the issue becomes more of a challenge. In the energy sector the concept of 'home' and 'host' country regulation is not apparent yet, but may become necessary not only around ECI designated assets, but CNI assets. This would not only ensure a level playing field in terms of the cost of implementing consistent security measures throughout the supply chain, **but also raise the profile and importance of the security of supply throughout the EU**.

A pre-requisite for a discussion about risk pricing is a knowledge of what the aggregate security risk exposure of an Asset Owner actually is and the costs involved in mitigating it across the supply chain, taking account of the different regulatory and legislative requirements in the countries involved in that chain.

In conclusion, in an increasingly volatile global risk environment, issues as important as security of supply and concerns about economic resilience are not going to go away. The interests of policy-makers and Asset owners need to be united and aimed at creating solutions that balance the needs of each for continuity and clarity. On the current trajectory, that is not going to happen and the potential cost implications will become far more significant – for government, for companies and consumers.

Stephen Gregory
Chief Executive Officer
Harnser Risk Group

Chapter 2
How to use the Guidelines

2 How to use the Guidelines

These Guidelines are for the primary use of owners and operators of energy infrastructure Assets in the EU.

However, given the global nature of the industry and the requirement of a Board of Directors for a single cost for implementing a **Corporate** Security Strategy, it is recommended that the Guidelines be applied on a Group-wide basis.

There are several individuals who need to take joint responsibility for applying the Guidelines and managing the outcomes.

These are the:

1. **Finance Director** as the individual responsible for managing the financial planning and investment appraisal process to approve and control expenditure.
2. **Security Director** or **Manager** responsible for identifying where and how security risk impacts on the company and who needs to be involved in implementing the Security Strategy.
3. **Strategy Director** as the individual responsible for developing and presenting strategies for consideration by the Board with the risks associated with each set out.
4. **Business Heads** as those individuals responsible for implementing the Corporate Strategy in line with the risk tolerance levels deemed acceptable by the Board for ALL risks. As such, it is also their role to ensure that the accompanying Security Strategy for their area of responsibility is implemented and that there is evidence of it being so.

4a. **Operations Managers** as a particular Business Head who are responsible for the sites and facilities. Often a significant budget-holder, these Managers have a keen interest in managing risk appropriate to the threat and will be responsible for the expenditure on physical and personnel security in particular. They are a critical stakeholder in any Security Strategy.

There are, of course, other individuals heading up departments who would be involved in applying the relevant sections of the Guidelines to their area, and those who are involved in planning, but the roles above are those accountable to the Board of Directors and key external stakeholders for ensuring there is a joined-up approach for implementing the Security Strategy.

Before the Guidelines begin, Chapters 3 and 4 explain what the impact of security risk can be across a business and how to develop a Security Strategy.

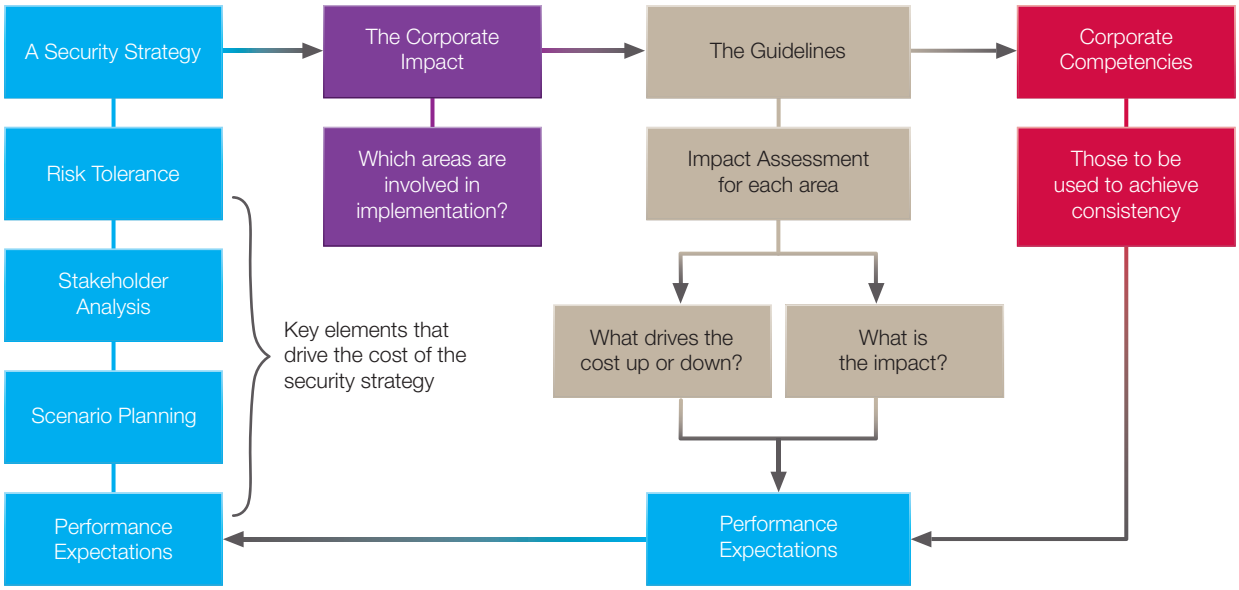
Identifying the financial impact of a Security Strategy comes at the end of a planning process and Fig. 2.1 sets out some of the key elements in that planning process that are of particular relevance to the overall cost of implementation.

The Guidelines can be distributed to the individual department heads for completion using a process similar to those used in business continuity planning insofar as an impact assessment needs to be done, inter-departmental relationships need to be identified, tolerance levels need to be established, actions identified and then costed and approved.

Each section relates to a specific area or department and includes a reference relating to process and performance, as well as a definition and explanatory note. The questions are laid out in tabular form with those on the left focusing on questions that will demonstrate those factors that will drive the financial cost or spend in that particular aspect. The right hand column explains why this matters and how to review a potential answer from the area or department concerned.

The structure of the Guidelines is shown below:

Fig. 2.1 The Structure of the Guidelines



It is the hope of the EC that the Guidelines will enable Asset owners to compare and contrast their own approach with that of their peers. Judicious benchmarking will contribute to raising awareness of where and how value for money can be achieved across the supply chain and this is to be encouraged. As noted earlier, for a competitive level playing field to work, the costs of doing business across the EU have to be streamlined – and this includes the cost of managing security risks.

Chapter 3
Developing a Security Strategy

3 Developing a Security Strategy

The purpose of the Guidelines is to aid the identification and quantification of the financial costs associated with the implementation of an agreed Security Strategy. However, not every energy company has a Security Strategy.

This section explains what a Security Strategy is and what it is not. It notes three areas of analysis that have a material impact on what the financial implications of implementing that Strategy is; namely a Stakeholder Analysis, Scenario Planning and Performance standards.

A '**Security Strategy**' is a document that **sets the context** for site specific **Security Management Plans** which focus on how the strategy is going to be implemented, **Asset by Asset**.

The Security Strategy relates directly to the Corporate Strategy and the Regional Strategy that follows as a result for the business as a whole.

Each Asset needs a specific Security Management Plan to reflect the local environment, local stakeholders and the characteristics of the Asset itself.

A good Security Strategy would:

- Take the agreed Corporate Strategy as its starting point.
- Confirm the Group's risk appetite or tolerance for losses.
- Identify who the key stakeholders are and why.
- Confirm the governance framework to be used to provide assurance to stakeholders.
- Explain the risk assessment process and reporting model to be applied.
- Set out the high level scenario planning assumptions based on a high level analysis of the security environment.
- Explain the risk assessment process to be applied at Asset level and how the outcomes from that process will evaluated and acted upon.
- Explain the monitoring and reporting model to be used.
- Define clear objectives for security risk management over the period of the Corporate Strategic Plan and explain the security planning process to be undertaken at Asset level to achieve them.

Although managing security risk requires the support and engagement of many areas in an energy company, few **have** a consolidated **Security Strategy** which defines what the **consolidated security exposure** is and the cost of managing it. It is therefore difficult for a Board of Directors to know the **security risk:reward trade-off** that is an inherent part of the strategic decision-making process. See Box 3.1.

Box 3.1.

Creating shareholder value requires a Board to balance the **opportunity of Reward with the Risk of loss** – they are two sides of the same coin. The strategic process links them together so that a Board can make choices about each. Often Strategic Plans cover a 3-5 year planning horizon. Whilst investment decisions in the energy sector can range from 5-30 years, it is impossible to plan strategically beyond five years without the planning assumptions being less reliable than markets would wish. However, even within five years change can be significant and the planning process has to be flexible enough to deal with it and react accordingly. If the process is robust, then opportunities can be pursued and risks re-evaluated quickly and effectively.

In the E&P sector, retaining a culture of 'entrepreneurship' is fundamental to most players as it has driven a great deal of shareholder value. Such companies need to ensure their strategic and risk planning processes allow for that culture to remain successful, without damaging the business.

By way of definition, the following are well established: One theoretical, the other practical:

Johnson and Scholes define strategy as: "..the direction and scope of a company over the long-term; which achieves advantage for the company through the configuration of its resources within a challenging environment, to meet the needs of markets and to fulfil stakeholder expectations."

Jack Welch, the former CEO of General Electric Corporation puts it more succinctly: "Strategy is a living, breathing, totally dynamic game…simply finding the big aha and setting a broad direction, putting the right people behind it, and then executing with an unyielding emphasis on continual improvement."

The Security Strategy has a cost to it and how each area responds to that Strategy depends on decisions made about stakeholders, senarios and performance. Each influences the choices made about implementing a Security Strategy and the costs involved.

3.1 Stakeholder Analysis

Energy companies operate in an increasingly complex environment and the range of stakeholders who must be communicated with on matters relating to security risk management has widened.

For the purposes of these Guidelines, a stakeholder is defined as those parties (internal and external) who have an interest in, and influence on the management of security risk. These stakeholders operate on a global, regional, national and local level.

Without effective engagement of and support from these stakeholders, the proposed Security Strategy and its financial implications will be difficult to manage and is likely to lead to:

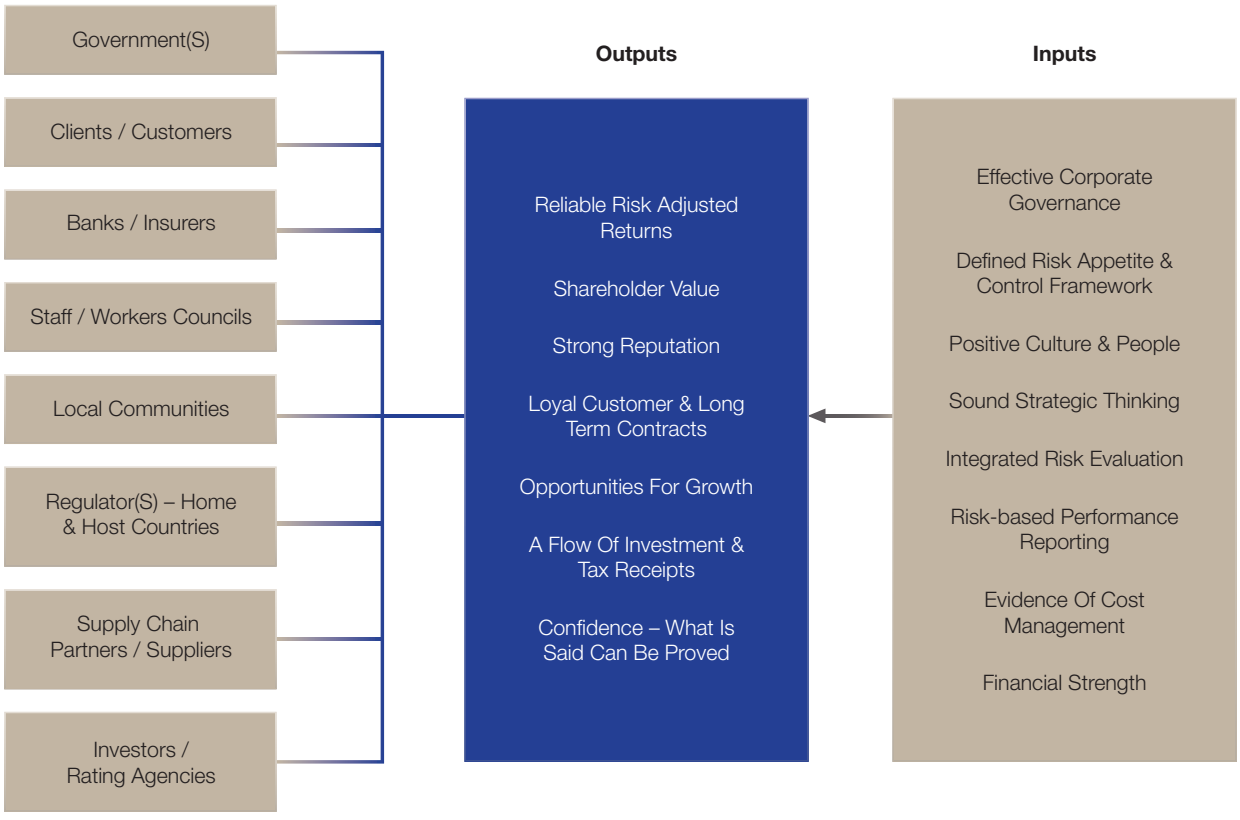
- Poor communication with stakeholders.
- Lack of support for those with security risk management responsibilities.
- Lack of approval and resourcing for security risk management activities.
- Difficulty in managing stakeholder expectations.
- Awareness of security risk issues remaining low.

Despite the range of stakeholders, fundamentally they are interested in the same results, as shown in Fig. 3.1.1 below.

The concept of Created Shared Value (CSV) is relevant here as it is based on the idea that corporate success and social welfare are interdependent. A business needs a healthy, educated workforce, sustainable resources and adept government to compete effectively. For society to thrive, profitable and competitive businesses must be developed and supported to create income, wealth, tax revenues, and opportunities for philanthropy.

CSV is also referred to in the **OECD Corporate Governance Principles** (set out in 5.2) where the importance of encouraging active co-operation between companies and stakeholders in creating wealth, jobs and the sustainability of financially sound enterprises is cited as a specific Principle. [1]

Fig. 3.1.1 Stakeholder Interests in Security Risk



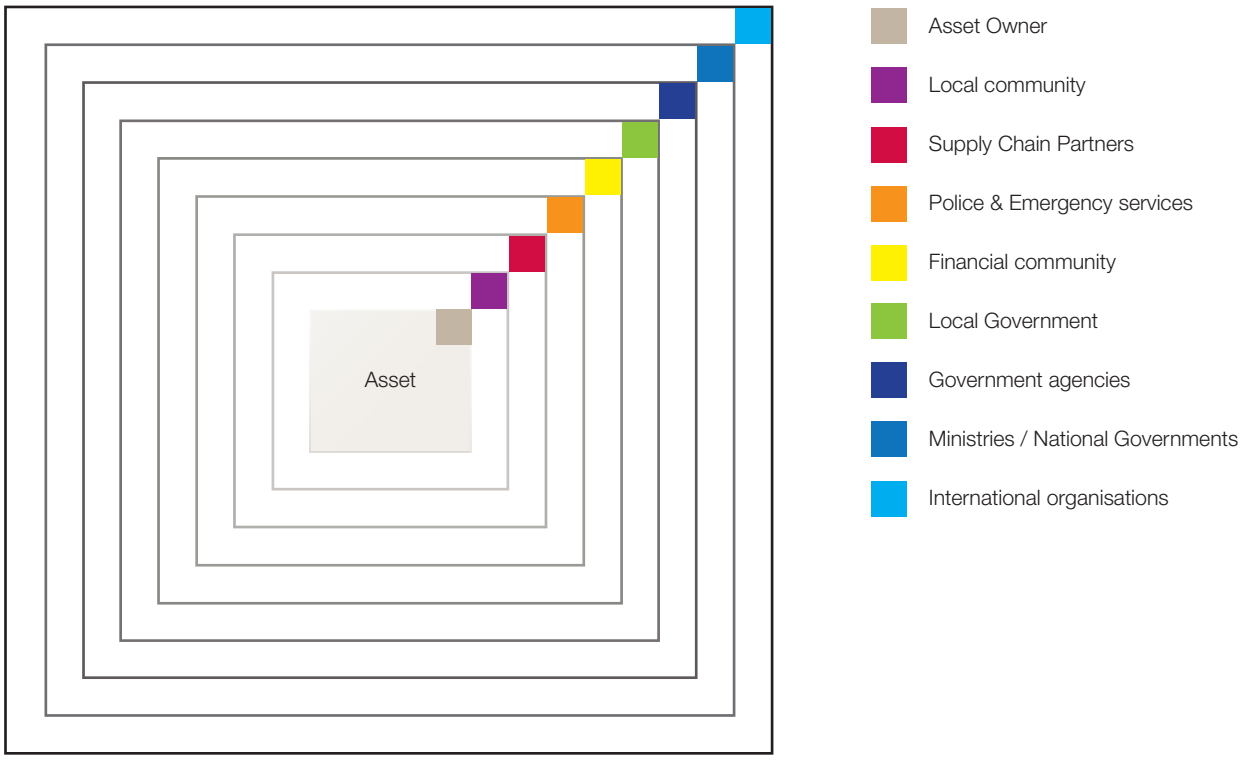
The breadth of dialogue on security risk has broadened in the last ten years. It is routine to talk to **governments** about CNI strategies for their energy sectors; to **banks** about the impact of security risk on financial returns; to **executive managers in E&P** companies about the sensitivity analysis that should be undertaken on financial forecasts and the impact of changing an operational model in response to security concerns; to **utility companies** about the management of contracts to implement protective measures, and the effectiveness of those measures; **emergency services** in emergency planning exercises; to **rating agencies** about security threats to creditworthiness; to **transnational organisations** about cross-border security issues; to all our energy contacts about **governance and regulatory expectations**; to risk professionals about how to understand the nature and impact of security risk on the energy sector; and to **investment and multi-lateral development banks** about the need for a security risk due diligence process.

This dialogue will increase as the need to ensure the protection and resilience of the energy sector grows around the world. This is a global issue. All have an interest in what the risks are and what the financial impact on governments, regulators and asset owners could be as a result.

For the Asset Owner, knowing who is dealing with what can be perplexing. As the issue of energy resilience grows, so will the layers of interest in how an Asset Owner fulfils its quasi-public and private sector responsibilities to the Outputs noted in Fig. 3.1.1.

Fig. 3.1.2 shows how this appears to an Asset Owner looking 'out' towards the stakeholders with an interest and influence over what they do around a particular site or facility.

Fig. 3.1.2 Stakeholder Interests in a Site or Facility



[1] *CSV received global attention in the Harvard Business Review article Strategy & Society: The Link between Competitive Advantage and Corporate Social Responsibility (1) by Michael E. Porter, a leading authority on competitive strategy and head of the Institute for Strategy and Competitiveness at Harvard Business School; and Mark R. Kramer, Senior Fellow at the Kennedy School at Harvard University and co-founder of FSG Social Impact Advisors.*

Tables 3.1.1 and 3.1.2 summarise the various generic internal and external stakeholders who have an interest in and influence on how a Company manages its Security Strategy and associated financial implications.

Table 3.1.1
Internal Key Stakeholder Overview

Stakeholder	Interest in Security Risk	Influence on Security Risk	Financial Implications
Board	Holds ultimate responsibility for security risk	Defining risk appetite and signing off on how security risk will be managed	Board approach dictates how the company treat, tolerate, terminate or transfers security risk
Head of Finance	Cost management of security risk	Able to sign off on the financial impact of security risks Conduct of financial cost:benefit analysis in accordance with corporate policy	Appropriate funding (or otherwise) of security functions including exceptional expenditure and structured programmes of investment
Head of Operations	Day to day accountability	Has to understand and support the rationale behind security risk planning Assess how changing security risk might affect operations Support for security department functions as a 'business enabler'	Budget holder and reports to corporate head office
Maintenance Department	Likely to be given non-technical aspects of security systems maintenance	Assistance in the upkeep of asset security systems	Effective 'in-house' maintenance will reduce call outs of bespoke contractors
Personnel Department	Hiring, training and dealing with staff	Vetting and screening issues for staff and contractors	Appropriate staff appointments made, staff retention, personnel security risks reduced and therefore reduced exposure to fraud, reputational damage, workplace crime and incompetency
Procurement Department	Services, systems, technology and materials related to security purchased via this department	May be required to sign off any request for financial resources from Finance department Purchasing decisions may be made on the basis of economy rather than necessity	Price negotiation, invoicing for payment, contract administration, value analysis, appropriate (or otherwise) security related purchases of equipment and services
Staff/Workers Council	Security of personnel, working conditions	Industrial/strike action, work to rule	Operational impact/ lost revenue, increase in asset exposure to security risk

Table 3.1.2
External Key Stakeholder Overview

Stakeholder	Interest in Security Risk	Influence on Security Risk	Financial Implications
Industry Regulator	Best practice, governance and strategy	May oversee Value For Money (VFM) process	Confirms/denies VFM met where government imposed security enhancement programmes allow cost recovery
National and host country Health & Safety regulators	Elements of security risk may fall under the remit of H&S regulators	Enforcement action, legislative obligations, conduct campaigns for improvement, will act in the public interest	Associated compliance costs
Government CNI agency	Acts as the government authority for protective secure strategy	May prescribe mandatory security standards, conduct inspections and surveys, set best practice, publish threat information, categorise/rank CNI assets	Requirement for financial expenditure to meet and maintain prescribed security standards
Emergency Services	Incident/emergency specific	Establish their requirements for emergency access, health & safety procedures, equipment, compliance with building codes and regulations, availability of response	Associated compliance costs including exercises, establishment of 'in-house' emergency capability where necessary
Police	Incident/emergency specific	Establish their requirements for security systems at asset(s), criminal activity of concern, availability of response	Associated compliance costs including exercises, extra security including technical, manpower, procedural
National government departments and agencies	Oversight of national security strategy and related policy/legislation	Strategic Frameworks and Policy Sector Specific Resilience Plans Counter Terrorism policy Oversight of CNI agency Delivery of security legislation	Requirement for financial expenditure to ensure compliance with legislative requirements
Local Community	H&S issues, fear of loss of containment, is the asset a target?	Demonstrations/ campaigns against the company and/or asset, blockades	Operational impact/ lost revenue, reputation, repair costs, cost of asset security improvements
Banks/Insurers	Due Diligence Impact of security risk on financial returns	Is security risk considered? Who owns the security risk?	Loss of lines of credit, inability to insure operations, increased loan repayments, increased premiums
Supply Chain	Concern about their own exposure to security risk	May bring pressure to bear on other operators in chain	Supply chain operators may not wish to continue doing business

As well as identifying stakeholders and their interests and influences on security risk, it is a worthwhile exercise to **prioritise** these stakeholders in order to identify those who are of most value to the security strategy and have the greatest influence on it.

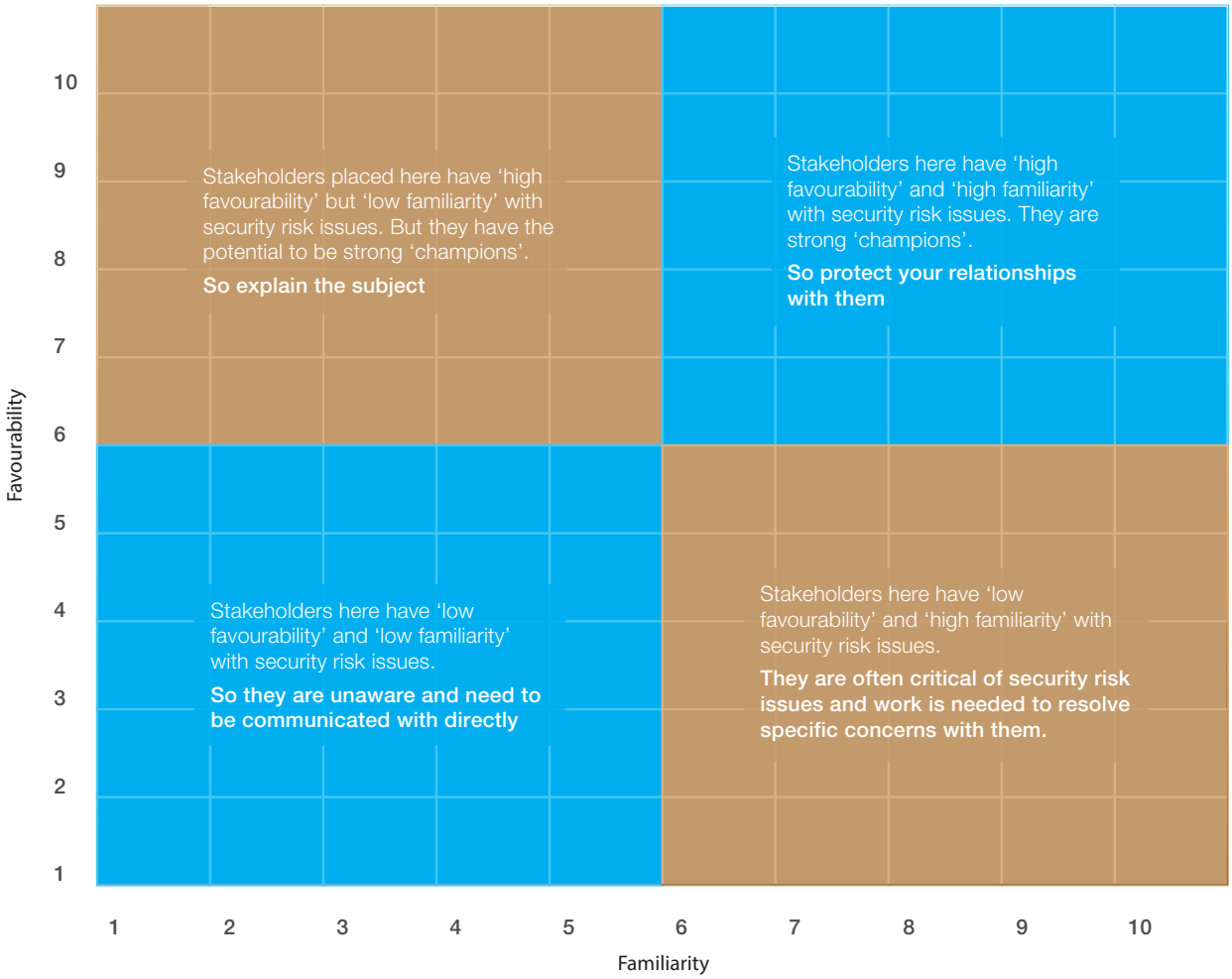
This will assist in the analysis of associated financial implications and determine approaches for how and when stakeholders should be engaged with. There are two fundamental elements involved in this as shown in Table 3.1.3 below:

Table 3.1.3
Stakeholder Prioritisation

Prioritisation Factors	Description
Familiarity	How well does each stakeholder understand security risk and what the Company's security risk strategy is seeking to achieve?
Favourability	How well disposed is each stakeholder towards the implementation and continued development of the Company's security risk strategy?

Using a matrix as shown on Fig. 3.1.3 below provides a method for determining levels of stakeholder familiarity and favourability.

Fig. 3.1.3 Stakeholder Familiarity and Favourability Matrix



Security threats are not immediately considered as stakeholders, but given that they are the reason for a Company's Security Strategy, and can have a direct influence on operations, it would be prudent to include them in the stakeholder analysis. These were summarised in Table 1.1 in Chapter 1.

In conclusion, given the number of stakeholders that have an interest in and influence on security risks, it is not surprising that there are a number of mutual interest between them. Table 3.1.5 looks at these from a financial perspective.

Table 3.1.5
Stakeholder Mutual Interests

Financial Implications	Interested Stakeholders	
	Internal	**External**
Board approach - treat, tolerate, terminate or transfer security risk	Board Head of Finance Head of Operations Personnel Dept Staff/Workers Council	Government Banks/Insurers Government Local Community Regulators Police/Emergency Services CNI Agency
Personnel security issues, exposure to fraud, reputational damage, workplace crime and incompetency	Personnel Dept	Police CNI Agency
Appropriate security related purchases of equipment and services	Procurement Dept Head of Finance	CNI Agency
Supply Chain exposure to security risk	Head of Operations	Supply Chain
Compliance Costs Legislative obligations Mandatory standards Funding Incident/Emergency capability	Head of Finance Head of Operations Procurement Dept	Government CNI Agency Police Emergency Services Banks/Insurers H&S Regulator
Loss of credit lines/insurances	Board Head of Finance	Banks/Insurers
Funding of Security Functions	Board Head of Finance Procurement Dept	Banks/Insurers
VFM/Cost Recovery	Head of Finance Head of Operations	CNI Agency Regulator Government Banks/Insurers
Maintenance Costs	Maintenance Dept Head of Finance Procurement Dept	Banks/Insurers
Operational Impacts Industrial action Lost revenue Reputation Shut downs	Board Head of Operations Head of Finance Personnel Dept	Local Community Workers Council Police/Emergency Services Government

To sum up, stakeholder interests and influence can dictate what an energy company needs to do to manage its security risk. **So taking account of those interests early on in the Security Strategy is crucial to managing the cost of implementation.**

3.2 Scenario Planning

Broadly, scenario planning is a tool for understanding potential future events and is designed to support decision making and planning cycles.

From a security risk management perspective, scenario planning serves to:

- Reduce and manage uncertainty.
- Identify risks.
- Show how events may unfold.
- Allow a better understanding of consequences.
- Highlight an organisation's vulnerability to events.
- Allow better organisational preparation including the design and implementation of mitigation measures and response procedures.

In a summary of what goes wrong in risk management Deloittes list that 'Probabilistic modelling was overemphasised; shortcuts were taken; scenario planning was underused; transparency into potential issues was absent'.

Source: Deloittes 2009 'Putting Risk in the Comfort Zone: Nine Principles for Building the Risk Intelligent Enterprise'

Within the energy sector, the use of scenario planning is becoming an increasingly important tool in risk management.

Furthermore, ratings agencies themselves are taking a keen interest in how companies manage security risk as part of the process for determining the level and cost of financing infrastructure investments.

The use of scenario planning in order to determine the link between risk and rating is therefore becoming an important factor.

Insurance companies also have an increased level of interest in how security risk is taken account of in all-risks scenario planning and how decisions about its mitigation are taken.

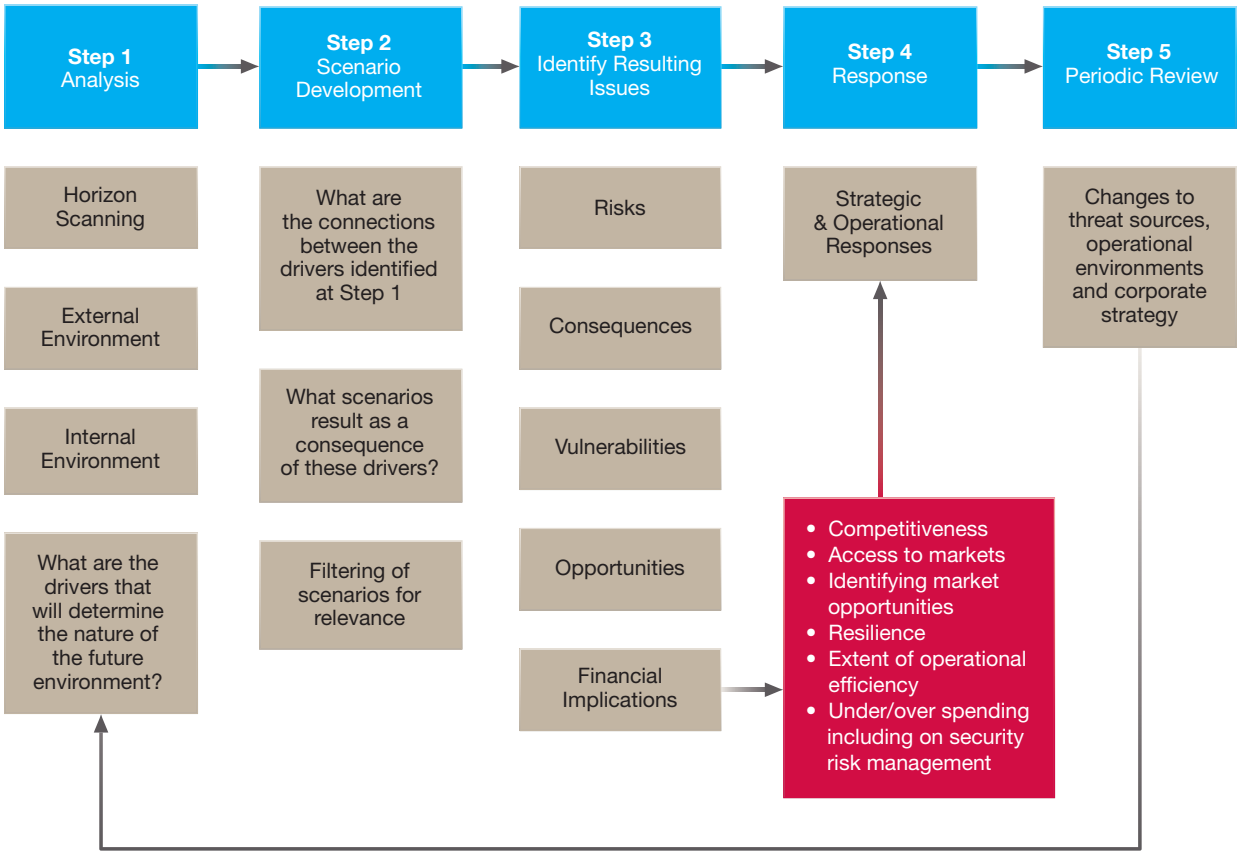
In conducting scenario planning, an organisation will have a better understanding of the possible outcomes that may result from pursuing its corporate strategy and the risks associated with doing so. By encompassing security risk scenarios within this process, the full impact of various outcomes on financial returns can be analysed.

Scenario planning can provide a methodology for considering potential implications of events, how a company might respond, highlighting organisational deficiencies and what risks and opportunities may result from certain events.

It should be noted that whilst scenario planning can provide a context of how operating environments may change and specific events unfold, it will not provide an organisation with predictions about what future events will materialise.

There are a number of different scenario categories that a company can use, an analysis of which is beyond the scope of this document. However, there are common steps to the scenario planning process, each of which has a number of considerations. These are highlighted in Fig. 3.2.1 below:

Fig. 3.2.1 A Scenario Planning Process



Threat scenarios are an important tool in the risk management process. Whilst a description of Security Risk Assessment methodology is outside the scope of this chapter, Fig. 3.2.2 highlights where the use of threat scenarios fits into a wider Risk Assessment process. The use of threat scenarios transform general threats into specific incidents and as such allow for a more detailed analysis of consequences, vulnerability and likelihood.

As a result organisations can decide specifically what needs to be protected from which type of threats, which subsequently provides the basis for the design of cost-effective and focused mitigation measures.

The potential disadvantage of using scenarios as the basis for risk analysis is that it is impossible to cover all eventualities and as such there is the possibility that mitigation measures may not provide complete protection. However, this is always a possibility and typically far more likely to occur when trying to protect against a threat in general rather than a specific type of incident.

In order to further reduce this risk and ensure scenarios are as representative of real-life incidents as possible, the following approach should be taken:

- Start with a wide range of scenarios based upon careful analysis of threat characteristics, and subsequently filter out those scenarios which are less relevant due to a lack of significant consequences, inherent vulnerability or likelihood.

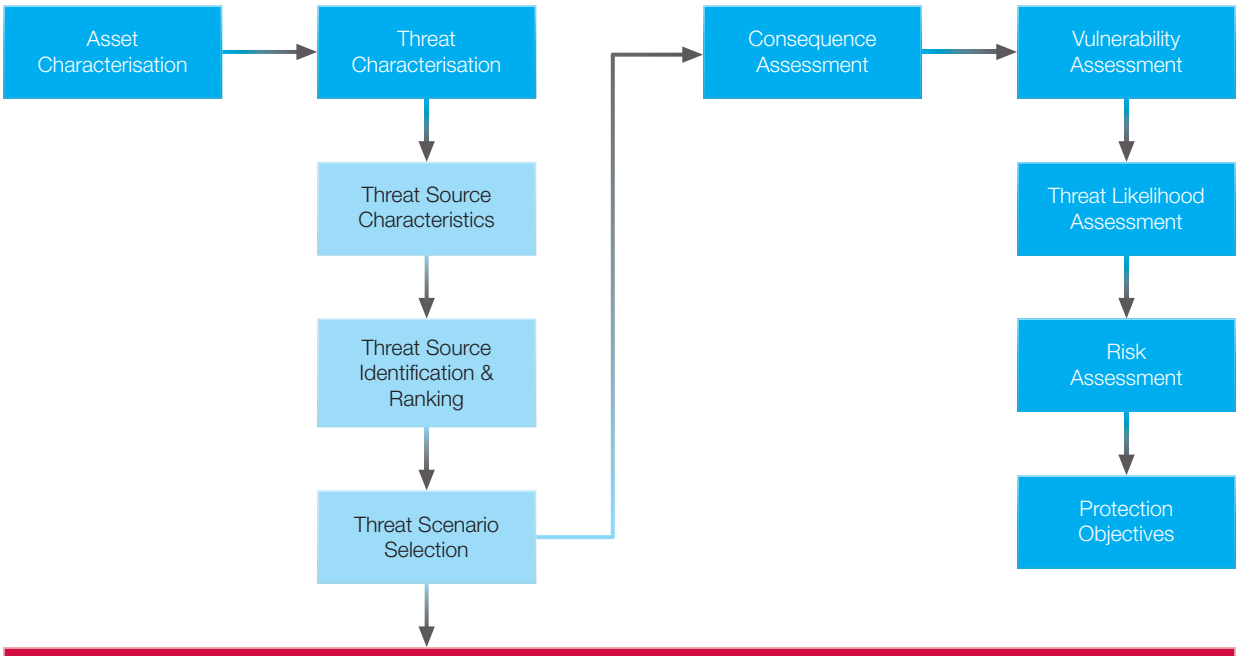
  As a result a wide range of possibilities can be considered, **but only the most relevant scenarios are captured for further analysis, which subsequently provides the basis for very focused mitigation options.**

- Use the scenario as the highest point of analysis, thus allowing each scenario to be considered in terms of the risk posed to all parts of the Asset deemed critical rather than just the Asset as a whole or a single component (when others may be also be at risk). **In effect this creates a number of sub-scenarios for each primary Threat Scenario.**
- Threat Scenarios need to be flexible enough to cover slight variations in the method of attack that may actually be employed, but not so flexible that they do not provide a useful analysis tool.

  The scenarios should however cover the main types of attack and possible targets associated with each Threat Source, since this is necessary to identify possible consequences of the threat materialising.

The use of threat scenarios when conducting security risk assessment should be given due time and attention by the project team and revisited on a regular basis, **and must be incorporated into the wider scenario planning exercise for identifying and considering all risks associated with particular strategies being considered by the Corporate Strategy department.**

Fig 3.2.2 Use of Threat Scenarios in Security Risk Assessment



Financial implications of using threat scenarios in security risk assessment:

- Will assist in developing cost effective and focused mitigation measures and thus avoiding expensive, unnecessary and convoluted mitigation measures (which in turn will require expensive and time consuming remedial works to put right).
- Will assist in the development of security measures that do not adversely impact on operational output.
- Will allow the development of security measures that are consistent with the corporate strategy and organisation's risk appetite.
- Will support security project design and help to minimise expensive and time consuming cost overruns.

Source: PRISM® Phase B

3.3 Performance

The Guidelines do not explain **how** security risks should be identified and mitigated; instead they focus on identifying the financial impact of the Security Strategy based on that analysis across the business. However, it is crucial that the Board of Directors have assurance that what they do decide to spend on the security of assets and infrastructure **actually delivers the reduction in risk expected. So have the measures delivered the level of performance expected?**

For that to happen, **there has to be confidence in the process** used to develop that Security Strategy – if not, how can there be confidence in what that process means on a Group-wide basis in terms of actions, investment and cost? **There can be none**.

As an example, if one looked at how large companies develop budgets, the process is a combination of top-down expectations and guidelines about how budgets should be constructed for each designated area – which might be by department, or location, or project – depending on the organisational structure of the company; with bottom-up proposals for how that area is going to contribute to the Group's Corporate Strategy in Year One of the Strategic Plan.

It is an iterative process, but a well-established one that all managers are familiar with and at its conclusion, the Board of Directors can sign-off on a budget that has the full confidence and endorsement of the Finance Director, who owns the process and knows it has been applied fairly and consistently across the business.

Security expenditure rarely has a defined budget of its own. It is usually part of another department's budget or, when a new project is being evaluated and the potential cost of security risk mitigation measures should be taken account of in the FEED stage, these would need to be quantified. This means that it is a) difficult to quantify the financial implications of a security strategy, hence these Guidelines; and b) impossible to know with any certainty about whether that expenditure will deliver the performance in risk reduction required.

So having confidence in **what the proposed security expenditure will deliver** is crucial to the cost:benefit analysis that should accompany the request. This might be described as the "**performance challenge**", but it is no different from how any area of expenditure might be scrutinised through the budget, or incorporated within the overall budget for a new development.

See box 3.3.1 for an explanation of how performance can be embedded into the security risk management process using a Performance and Risk-based Security Methodology called PRISM®.

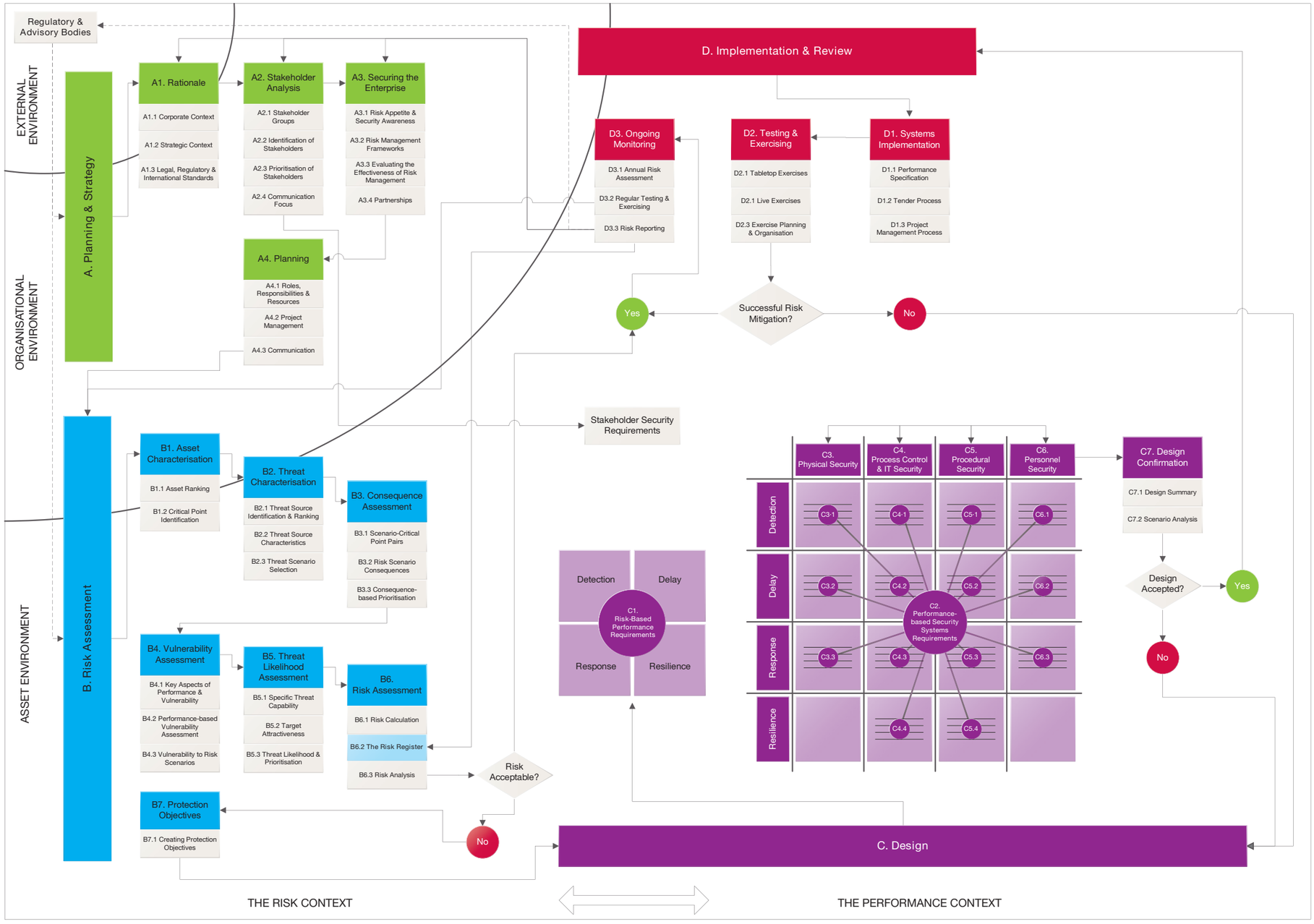


Figure 3.3.2
The PRISM® Process

Box 3.3.1. PRISM®

This process was written into the Reference Security Management Plan (the "RSMP") for energy owners and operators. It is a complete security risk management process that can be applied on a consistent basis to any site, anywhere in the world. Reflecting the unique environment of the asset or programme the process is applied with measurable outcomes and results linked back to aims and objectives.

The process sets out a logical and methodical approach to good risk assessment, design and implementation, ensuring that the outcomes are embedded into the key planning and risk management activities in the company concerned. It can sit alongside the corporate and business strategy planning process so that it can link decisions at the top about risk tolerance and governance to tangible outcomes on the ground. So it forces users to make decisions, justify those decisions and leave an audit trail – so the benefits of expenditure can be identified in terms of performance attained and risk reduced. It also has the additional benefit of supporting a value for money audit process on many aspects of physical and procedural security.

Box 3.3.2. Risk-based:

- An understanding of the specific risks facing each facility
- Scenario-based providing a clear output in terms of specific security incidents or attack methods that need to be mitigated
- Risk considered at the component as well as site level to focus on specific critical components and processes which must be protected
- Scoring that enable specific Protection Objectives to be derived

Performance-based:

- The level and type of performance required to mitigate specific risks
- Allows users to understand and identify their unique performance requirements in the areas vital to effective security the core functions of which are:
  - **Detection**: The ability to detect that an incident is occurring, assess the type of incident and the necessary response.
  - **Delay**: The ability to delay attackers or protect against the cause of the incident long enough for a successful response to be initiated.
  - **Response**: The ability to respond effectively to the incident, preventing loss or damage to the Asset by successfully intervening before it is compromised.
  - **Resilience**: The ability to mitigate the potential consequences of an incident either by resisting damage or recovering quickly from the consequences.

Source: The Reference Security Management Plan (RSMP)

Fig. 3.3.2 Targeting Performance through PRISM®

Chapter 4
Understanding the Impact of Security Risk

4 Understanding the Financial Impact of Security Risk

The impact of security events or incidents on a Company can be wide-reaching with serious consequences.

One of the challenges made to security risk practitioners is that 'it will never happen' and until an incident similar to Piper Alpha or Macondo happens as the result of a security incident, many are sceptical that security risks will occur and have a material impact on their business.

The answer is that given the impact and consequences to energy assets and infrastructure, as well as the growing obligation of a Board of Directors to demonstrate duty of care and the responsibilities that go with it, **how can a Board NOT make an informed decision about its stance on the extent and management of the security exposure it has agreed is acceptable for its people and assets?**

To choose not to do so is fundamentally at odds with Corporate Governance standards, regardless of management style and country of incorporation.

Global energy companies that choose to 'behave' differently in one location because local standards are less than those in their country of incorporation, or decide to "outsource" the management of security risks to a third party without satisfying themselves that the risk is being well managed, are taking a very serious risk indeed.

A security event or incident can do ALL of the following and the relationships between each are self-evident – the domino effect can be swift and far-reaching.

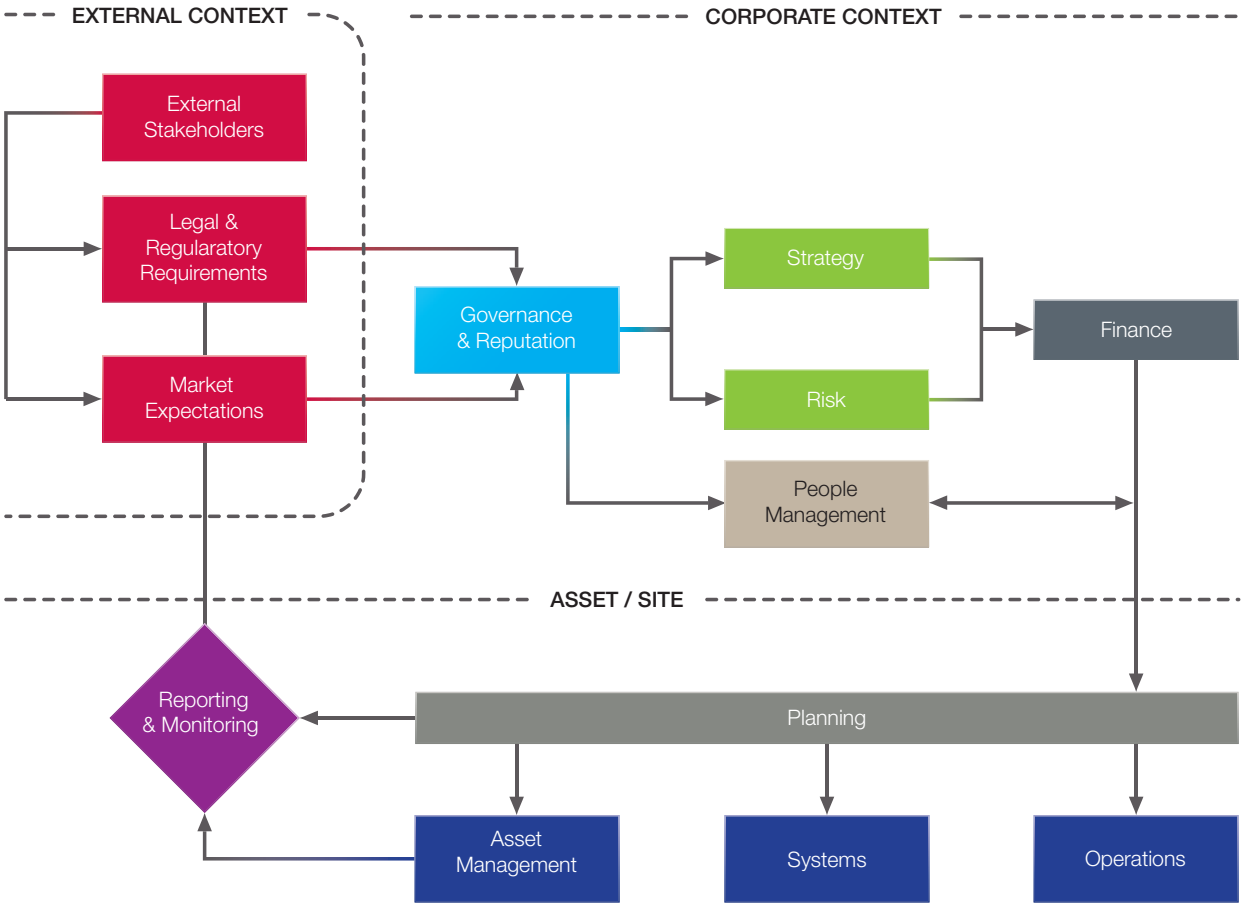
- Damage to company assets
- Disruption of technical operations (interruption of service/supply)
- Intrusion in corporate information systems
- Distortion of commercial operations
- Erosion of corporate image
- Health hazards to people
- Hazards to environment
- Propagation of disruption/damage to third parties assets and/or operations.
- Compliance and legal risk
- Limited access to partnerships (i.e. some may be excluded because of security concerns)
- A breach of Governance and internal control standards
- Closure of strategic opportunities
- Loss of earnings
- Increased Government and regulatory scrutiny
- Increased cost of funding from third parties
- Increased cost of insurance
- Credit rating downgrade and the impact on cost of debt and access to debt capital markets.

The departments involved in implementing a Security Strategy to make sure there is as low as reasonably possible chance of such impacts occurring are numerous. The Guidelines seek to cover all these departments. These are set out in detail in Chapter 5.

The following diagram shows the structure of the Guidelines and the areas they cover.

Almost all energy companies, irrespective of organisational structure and/or business model will have the same departments. At asset level, the types and location of facilities will, of course, vary depending on which sub-sector or part of the supply chain the company operates in.

Fig. 4.1 Areas of Impact



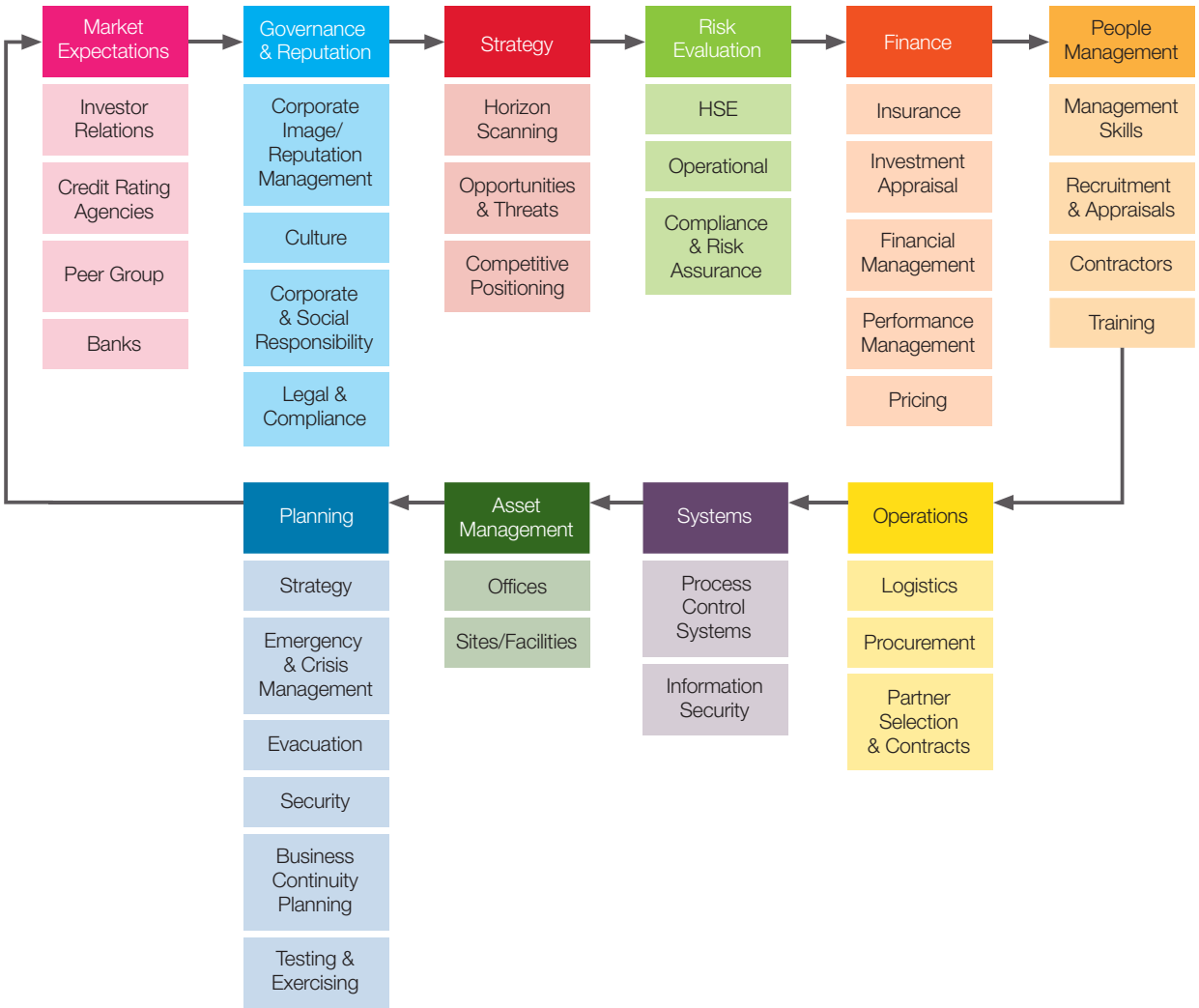
Chapter 5
The Guidelines

5 The Guidelines

This and subsequent subsections form the Guidelines. Fig. 5.1 is a detailed Impact Map of all the areas of corporate activity involved in implementing a Security Strategy.

The Guidelines include the external context dictated by Market Expectations and Legal and Regulatory requirements before moving onto the areas of activity which feature in all energy companies, even if the name of the department involved might differ slightly. Each of the areas noted in Fig. 5.1 are covered in detail in the sub-sections below.

Fig. 5.1 Impact Map



As noted earlier, the Guidelines are designed to be used as a set of questions for the Finance Department, along with the Security Director or Manager, to ask of each department.

Please note: 1. At the top of each area there is a reference to the **likely visibility of the issues raised** in that section within an energy company, from which one can infer the level of involvement, or otherwise, of the Security Director or Manager. This should be interpreted as follows:

Low	Medium	High
Low visibility and awareness within the Company - difficult to get answers to questions	Reasonable visibility and awareness within the Company - answers may be easy to obtain	High visibility and awareness within the Company - answers likely to be forthcoming

2. T**here is also a comment regarding the results or performance a Company could expect to see as a result of an investment in the area concerned**. See Chapter 3, sub-section 3.3 for an explanation of these, but it is important to remember that for some of the areas in the Guidelines, the money to be spent in implementing the Security Strategy may deliver intangible results that do not lend themselves to quantitative measurement. **In these instances, the outcomes for those areas need to link directly back to specific objectives**, otherwise it is impossible to demonstrate that money spent has achieved any of the benefits intended, and that is not acceptable from a financial or governance perspective.

5.1 Market Expectations

Market Expectations influence the scope, depth and cost of a Company's Security Strategy from the perspective of Investors (including analysts), Credit Rating Agencies and Banks who together influence the share price of, and cost of funding for, an energy company.

These are influential stakeholders with the ability to probe, challenge and benchmark how a Company manages risk against that of its peers.

Being aware of what their interest in security risk is, and why, will influence thinking about the risk profile of the business, now and in the future.

In other words, **the Board of Directors needs to know how much of a priority security risk is for each stakeholder and respond accordingly.** The relevance of this is reinforced in 5.2 on Governance and Reputation.

Fig. 5.1.1 shows the key elements that influence a credit rating and is provided by Fitch Ratings who have contributed to the Study in an advisory capacity. It is worth noting that many of the factors are common to investors and banks, the lines of enquiry to the contact points within an energy company will also be similar.

Fig. 5.1.1
Key Rating Factors

Key Rating Factors	
• Industry risk • Operating enviroment • Company profile • Management strategy/governanace • Group structure	• Financial profile - Cash flow and earnings - Capital structure - Financial flexibility

Source: Fitch Ratings

AREA OF IMPACT:
MARKET EXPECTATIONS

5.1.1 Investor Relations

Visibility			Performance
Low	Medium	High	Evidence that the potential impact of security risk on the Company's financial results has been acknowledged by analysts based on information provided by the Company in its results presentations and Q&A sessions.
		X	

Definition & Comment

The Investor relations team manage the dialogue with shareholders and are instrumental in supporting access to capital markets. They are the conduit through which questions are raised, and answered, about all aspects that influence the share price. As the single biggest threat to that share price, risk is a frequent agenda item, but the extent to which that includes security risk, is something every Company needs to ascertain.

The questions posed below will identify the level of awareness and interest in security risk management from investors, who are likely to be a very disparate group ranging from myriad individual shareholders, private equity groups to large pension funds. The Investor Relations team will know who the shareholders are and the questions they ask.

Financial Drivers	Impact & Implications
What are investor expectations about the Company's management of security risk?	Is security a risk investors have ever asked about? What assumptions do they make about it?
Has share price volatility ever been attributed to concerns about the security exposure in the Company's portfolio? Have security related risks had an impact on your ability to access capital markets and indirectly on your liquidity profile and capital structure?	Correlating share price moves to publicised security threats cannot be done with sufficient confidence, but an event which has a clear financial impact on a Company can impact on investor perception of risk. Something most Companies will seek to mitigate.
What type of information and reporting are investors given about risk management?	If there is any interest expressed, how much detail do investors require to be satisfied that what they are told, happens on the ground?
Are key security threat scenarios and mitigation incorporated into investor presentations?	A strong understanding of security risk and mitigation by analyst and investors can help to build their comfort level in the Company's ability to deal with threats and reduce price volatility in the appraisal value from communicated security risks occurring.
Does the Company state any security risk related items in its disclosure statements under Risk Factors?	Unmitigated risk factors are part of public disclosure processes for traded companies. Are there any security risk threats which are a part of such a disclosure? Does the Company have a process in place for the review of such risk factors and are these often picked up by analysts and investors as **non-mitigated risks** which can lead to appraisal value volatility on occurrence or threat thereof?

AREA OF IMPACT:
MARKET EXPECTATIONS

5.1.2 Credit Rating Agencies

Visibility

Low	Medium	High
		X

Performance

Evidence that the solicited ratings sought by the Company reflect (i) an acknowledged understanding of the security exposure inherent in the business and it's potential impact on creditworthiness; and (ii) knowledge of how that compares with the peer group the company is placed in.

Definition & Comment

A credit rating is a reflection of the Company's ability to service its debt (interest and principal) in full and on time – so it's 'creditworthiness'. It influences the ability to, and the cost of, raising debt on the debt capital markets. Typically, the higher the rating the lower the cost of funding which might be sought by a Company to fund either a specific Project or Development, or for more generic growth or restructuring opportunities. Market access also tends to be more predictable for higher rated entities with a predictable cashflow profile. **Ratings are not indicators of stability or confidence in companies or countries**.

There are a number of Credit Rating Agencies in the world and many of the larger energy companies will have ratings from several. Whilst their areas of interest may be similar to those of Investors and other energy sector credit and equity analysts, typically a Company would spend at least a day with each rating agency asking detailed questions to allow the agency to form an accurate picture of a Company's creditworthiness and the Executive Management's ability to sustain, or improve it.

Financial Drivers	Impact & Implications
To what extent is the security risk view of the agencies evident in the rating?	How well informed the agencies are about security threats that could jeopardise their assessment of creditworthiness will influence their interest. **In one sense, this is also a question of how closely aligned the rating is to its underlying threats**.
Has the Company's rating ever been altered because of a security event (or the consequences of it) or because of efforts that have been taken to reduce the risk?	If this had occurred, it would be known to the Company and its stance towards disclosure and discussion about risk management would therefore reflect the agency's interest and concerns.
Do rating agency presentations contain communication of security threats and mitigation?	An understanding of security threats, potential risks and mitigation efforts help a rating agency build comfort in the rating. It also drives a structured discipline for management review of the same and can drive decisions to cause a Company to spend money on security.

AREA OF IMPACT:
MARKET EXPECTATIONS

5.1.3 Peer Group

Visibility

Low	Medium	High
		X

Performance

The profile of the Company's Security Director/ Manager in industry groups and its engagement with government agencies reflect how others perceive the Company's approach. Being a 'Leader' or a 'Follower' is easy to discern given the relatively small number of players who decide to have 'a voice' on security matters at national or trans-national level.

Definition & Comment

Energy companies, depending on their areas of operation, often work collaboratively to reduce vulnerability. Whilst the concept of a 'level playing field' is one that has yet to be discussed openly by policy makers, at an operational level it is possible to save money by working in collaboration, and also to ensure that a security stance does not increase an exposure inadvertently – simply because a fellow player decides to manage their exposure differently.

By its very nature, security risk does not lend itself to benchmarking and there are no standards although there are guidelines issued by countries like the United States. So how a Company Security Director or Manager deals with security threats to corporate assets will depend on their own experience and network. Being aware of whether you are more or less exposed than your competitors, and whether that has a financial consequence to it, is not easy to determine. The following questions are designed to assist but undertaking a benchmarking exercise with peers on different aspects of their security risk management approach is to be encouraged.

Financial Drivers	Impact & Implications
Are there security sharing arrangements in place with other partners in a locality?	How does this work in practice, what assumptions are made about who will do what and how are the costs shared? Have the legal implications of such an arrangement been considered?
How does the Company's own approach to security differ from its competitors? Has it ever participated in peer group reviews?	At the moment, a Company can decide how it wishes to manage its security risk. It might follow guidelines depending on what sub-sector it operates in, or the advice of the national security service, if available. It is the decision of the Board and one of the factors that will influence their thinking is 'what do others do'? No company ever wants to spend more on any risk than it has to, however, anonymous peer benchmarking helps with information sharing and is a way to drive towards best/minimum standards.
To what extent does the Company view security risk as a competitive advantage?	E&P operators can be characterised as entrepreneurial and for that to be sustained, risk has to be managed well to support risk-taking activities. The risk:reward trade-off is managed actively, but how far does that extend to security where the consequences are more far-reaching?
Does the Company have processes to share common site risk vulnerabilities and threat scenarios with peer groups to understand interdependencies and ensure common risks are understood?	Interdependencies are critical in security risk assessments. It provides the basis of identification and the potential for resource sharing to reduce mitigation costs.

AREA OF IMPACT:
MARKET EXPECTATIONS

5.1.4 Banks

Visibility

Low	Medium	High
	X	

Performance

Evidence in the dialogue with the bankers of their awareness of the security exposure in the business and how it might affect their exposure to the Company. Whether in competitive syndications or specific project finance – have the security questions been asked and if not, does the Company know what assumptions have been made, but not raised?

Definition & Comment

As providers of finance with a track record of credit risk assessment, the banks **should be** well placed to evaluate the impact of security risk on the price and provision of finance. However, the extent to which they do so is unclear.

This reflects a number of factors. First, a lack of knowledge of the risk and how to place it into a credit assessment process; second, the pressure to write business in a competitive market; third, no established security risk due diligence process; and fourth, a wish to avoid complicating the credit process. So, perhaps surprisingly for a highly risk regulated industry, an energy company may find that their bankers do not know about its security exposure and how it impacts on them.

It would be prudent to establish the extent to which security risk is reflected in the price of commercial banking facilities or project finance, so that both parties can agree on how best to manage it.

Financial Drivers	Impact & Implications
Do you see differences between the assessment of banks and bond investors when evaluating security risk as part of their credit assessment?	Bond investors should be less reticent in their questions, what is the Company's experience?
How frequently does the Company change its bankers and why?	The longer relationship, the greater the level of knowledge about the business, the management and track record. In many countries, the nature of the banking relationship has changed to such an extent that such matters do not outweigh the potential for a company to get the best price for its funding.
Do banking presentations contain communication of security threats and mitigation?	An understanding of threats and mitigation give comfort to banks about the process used and applied in a company. As with questions from other stakeholders, this should support a structured discipline for management review of security risk, but there has to be an imperative for doing so.

5.2 Governance & Reputation

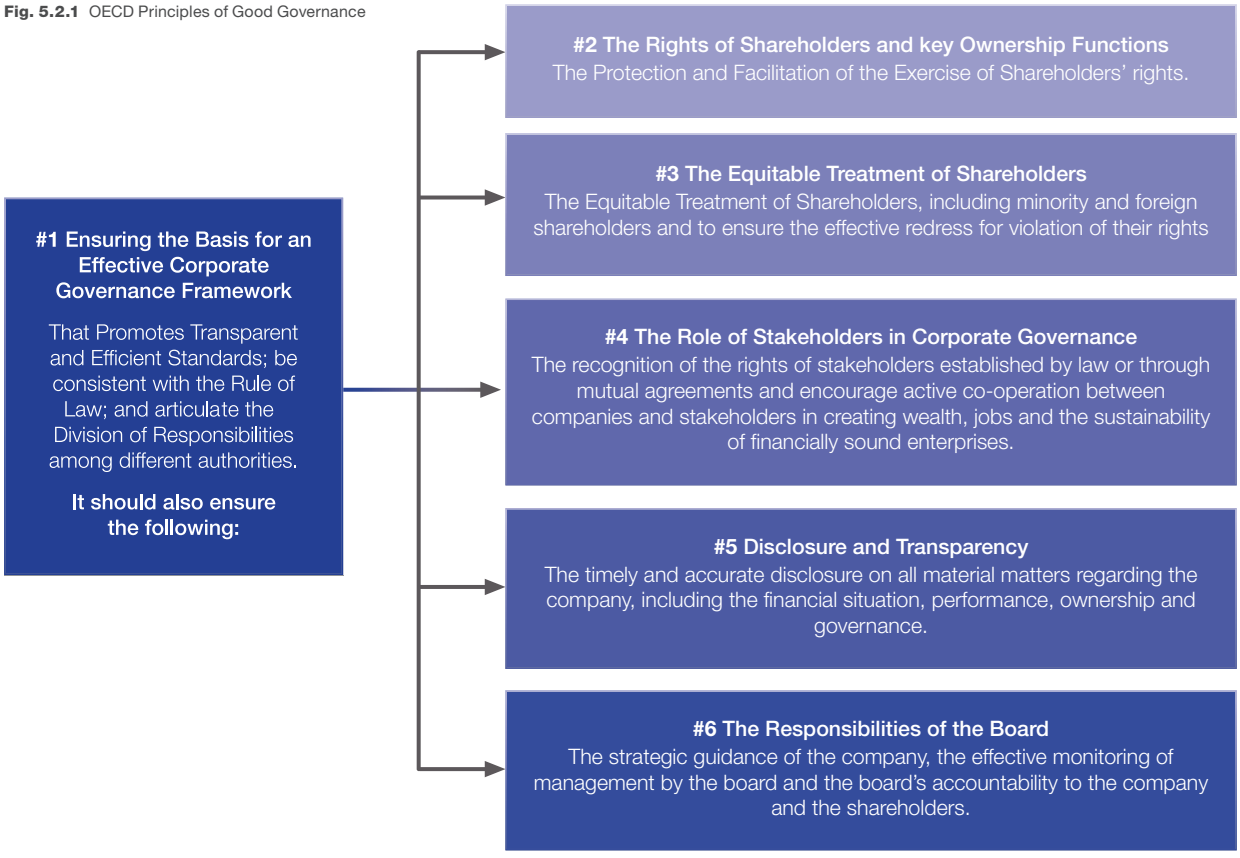
Governance and reputation influence how a Board of Directors thinks about security risk. The risk landscape as described by the World Economic Forum in its annual Global Risk Report points to the importance of good governance in assuring ALL stakeholders that a Board is able to fulfil its obligations to direct and control the business.

Corporate Governance is defined here as **the framework of rules, laws and processes that oversee how business activities are undertaken by an organisation** and as a reference, the OECD Principles of Good Governance are set out in Fig. 5.2.1.

As noted by the OECD, there is no single model of good corporate governance, but work carried out in both OECD and non-OECD countries and within the Organisation identified a number of common elements that underlie good corporate governance and which will be familiar to the reader.

The following areas are those involved in implementing the governance 'ethos' of an organisation and where costs can be incurred in implementing a Security Strategy. The expected outcomes are likely to be qualitative and preventative in nature, but this applies **to all outcomes** and not just those related to security.

Fig. 5.2.1 OECD Principles of Good Governance



AREA OF IMPACT:
GOVERNANCE & REPUTATION

5.2.1 Corporate Image/Reputation Management

Visibility

Low	Medium	High
	X	

Performance

This is an area where the benefits of investing in a Security Strategy are difficult to quantify. However, if taken together with Market Expectations and Partners, the responses given here will demonstrate to what extent expectations about the management of security risk are reflected in the Company's reputation.

Definition & Comment

Corporate reputation reflects the overall estimation in which a Company is held by its internal and external stakeholders based on its past actions and probability of its future behavior. A Company may have a slightly different reputation with each stakeholder according to their experiences in dealing with the Company or in what they have heard about it from others, but in general, companies seek to have a visible and consistent reputation with all who are aware of it, and engage with it.

Security risks can threaten reputation, but they need not damage it – that depends on the response of the Board and Management Team to a security incident or event. If a Board of Directors believes that the reputation of the Company is based, in part, on **their management of security risks**, then having a well-funded Security Strategy that delivers good management is important to how the Company is perceived externally.

Financial Drivers	Impact & Implications
Does the Board consider its security exposure as an influencing factor on its reputation? Should it?	This might be evident in how strategy is developed and discussed – an active risk-taking approach should imply a consideration of the impact of that approach on reputation.
To what extent does the Company's reputation reflect a competency or capability in security risk management?	This might be evident from the questions posed by those mentioned in the Chapter on Market Expectations, but also from interaction with other stakeholders. From this, a Company can determine whether it needs to strengthen its reputation in this area or not, using the corporate communications and investor relations teams.
Is there a corporate standard for security risk signed off by the Board?	If this exists, it sets the tone for how the risk should be perceived and it will provide a benchmark from which the risk infrastructure for security should flow. This will need to allow for local jurisdictions, but should not fall below the group standard. **The failure to have a security risk framework applied consistently across all assets means that a Company has no idea what its aggregate security exposure is, no assurance that the risks are being managed properly, that dependencies and consequences are being identified, and that reporting is based on the same fundamentals.** The management of any risk, if fragmented, is reliant on individual experience, locally driven, not only prevents any corporate competency or capability from being established, it is costly to maintain as no economies of scale are possible and a sense of unease about the risk, causes questions that few can answer.

AREA OF IMPACT:
GOVERNANCE & REPUTATION

5.2.2 Culture

Visibility

Low	Medium	High
		X

Performance

Evidence of a security culture can be sought in the same way the HSE culture is 'tested'. Often by means of a survey, or the use of mechanisms used to report near-misses, or observable failures of processes and procedures. In many energy companies, senior management will have a feel for the safety culture in the business and with that often used as a benchmark, it is usually possible to gauge how the security culture compares.

Definition & Comment

Corporate culture refers to the shared values, attitudes, standards, and beliefs that characterize members of an organization and define its nature. For many energy companies, a reference to 'risk culture' usually means HSE risks. This is a reflection of the visibility and investment within the sector over many years to create and sustain a HSE culture aimed at reducing the risk of incidents occurring.

Although security is linked to HSE as a cause and consequence, **it has not had the same level of investment and levels of awareness are measurably less as a result**. A security aware culture is in itself a strong preventative measure which can be achieved at a relatively low cost, but with high impact. So the challenge for any energy company is to know **how much it wants to invest in creating that visibility and why it would do so**.

The following questions will indicate how well established a security culture is and how it will be sustained. Culture is an intangible area, but it is manifest in the actions people take and the processes set out to direct and influence those actions - **so it is possible to find evidence of a culture working, or not**.

Financial Drivers	Impact & Implications
Is there an in house program that sets the tone from the top with regard to security to ensure it is part of the Corporate 'DNA'?	Smart communication programs help communicate and reinforce culture. Whilst it can be expensive to develop a security-focused corporate communications program, the Company will most likely already have a team in place with an ongoing communications infrastructure that simply needs to be aimed at security.
How would a member of staff or a contractor identify and describe the security culture or level of awareness in the Company? How often is this monitored?	If this is below what is expected, the Company needs to define the level of awareness it wants to achieve and how it wants staff and contractors to act as a result of that awareness.
Does the culture of the company encourage staff to be open about a change in circumstances or concerns they have? What mechanisms are in place for staff to share concerns/seek help?	A company that has invested in a strong welfare culture, perhaps with access to professional support, has an additional layer of mitigation that can capture and deal with events that could put an individual under pressure. This should be dealt with by the Personnel or HR department. For example, line manager contact, reporting hotlines (once approved by the Legal department), staff representatives.
What is done to ensure that new staff, contractors, partners understand the security culture of the Company?	The Induction process should deal with new employees, but there needs to be a formal process for doing the same with contractors, and any partner due diligence must include a review of security awareness and culture. Different expectations, experiences etc bring an increased level of risk to the Company that it needs to know about and deal with.

AREA OF IMPACT:
GOVERNANCE & REPUTATION

5.2.3 Corporate & Social Responsibility (CSR)

Visibility

Low	Medium	High
	X	

Performance

Measuring the results of CSR programs requires looking for indicators that demonstrate the outcomes meet the objectives set for the programs. These will differ, but must be noted even where the potential benefits need to be measured in decades, rather than years. In security terms, they need to achieve the same aim – to create a secure environment in which the Company can deliver its strategy, however long term in nature.

Definition & Comment

Corporate & Social Responsibility (CSR) is also referred to as 'corporate conscience', 'corporate citizenship' or 'responsible business'. It is a form of corporate self-regulation integrated into a business model whereby a business monitors and ensures its active compliance with the spirit of the law, ethical standards and international norms. Through its CSR programs a Company may expect to have a positive impact on the environment, consumers, employees, communities, and all other stakeholders.

Many energy companies recognise the value of a targeted and sustainable CSR program as a form of risk mitigation around its assets, both in its home country as well as host countries. Most relate to managing the environment around the Asset/facility to ensure a positive response from the local community and create an atmosphere where, should there be security challenges, the Company would be made aware of it through the channels of communication it had fostered and be in a position to respond appropriately.

So the questions for those responsible for CSR within a Company will show to what extent security risk mitigation features as an objective for one or more CSR programs and what might drive the level of cost up or down as a result.

Financial Drivers	Impact & Implications
To what extent are security considerations evident in the purpose and objectives of Company CSR programs?	What approach is used to develop and implement programs around critical assets? How is their effectiveness measured?
Is there a community relationship management or interface team to ensure awareness of assets and the security risks to those assets from the community?	Has the Company developed a structured and targeted process to create this awareness? For example community outreach and contact points for suspicious activity. This will manage potential threats and reduce any risk to acceptable levels at relatively low cost.
How would the Company describe its community relations around its key assets?	Past problems with the local communities (for whatever reason, for example, environmental concerns) or an increase in visitors to the surrounding area for reasons that could pose a security threat will undoubtedly influence a Company's stance.

AREA OF IMPACT:
GOVERNANCE & REPUTATION

5.2.4 Legal & Compliance

Visibility

Low	Medium	High
	X	

Performance

In this area there will be policies, processes and procedures that have to be adhered to by the business. Evidence that this is so will be subject to internal, and external, audit. However, the extent to which this governance framework applies to security risk will need to be established. Not every energy company will cover security risk from this perspective and knowledge across the business of how this affects their activities may be low. A Group-wide review to identify the Company's exposure to security related laws and regulations will generate objectives that can then be monitored.

Definition & Comment

The number of laws and regulations governing, and influencing, security around energy assets and infrastructure is growing. For example, in relation to corporate manslaughter, bribery, data protection, human rights, investigatory powers, offshore installations, whistle-blowing, dealing with hazardous materials and numerous safety regulations as well as sanctions. Maintaining an up to date knowledge of this, and ensuring compliance across all locations is critical, can be costly in terms of money and reputation, certainly if found to be in breach of any.

The questions should give an indication of how security risk is being managed from a legal and compliance perspective and where no or further investment might be required to deliver the Security Strategy.

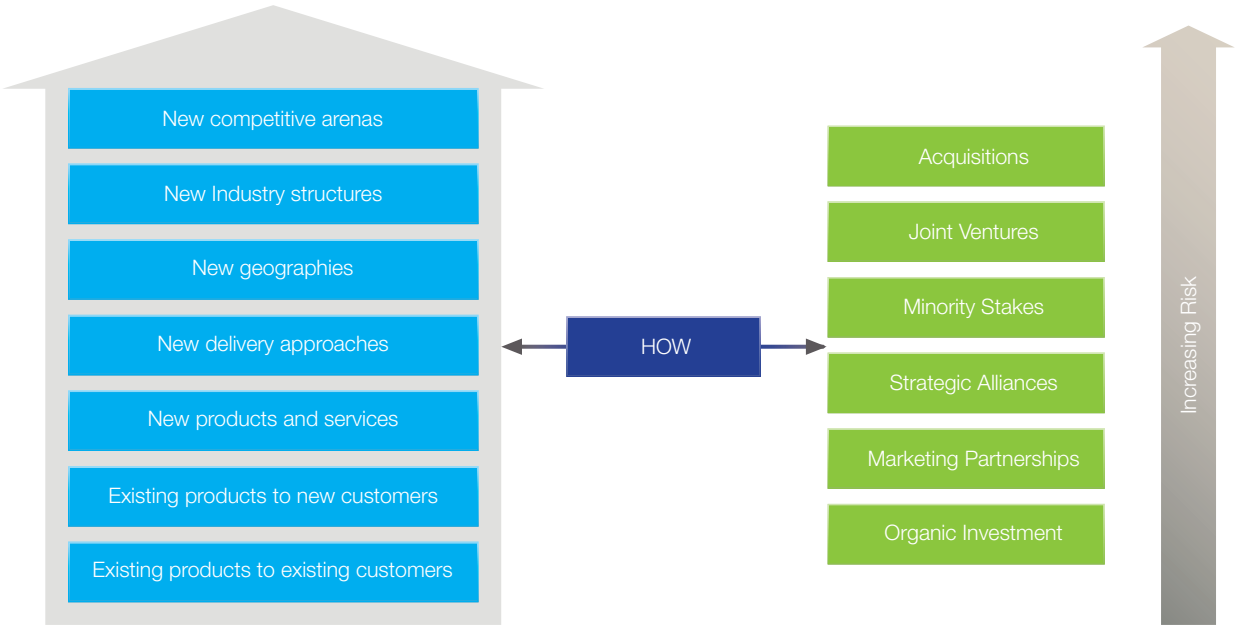
Financial Drivers	Impact & Implications
Is there an annual compliance review of the Company's adherence to all relevant security laws and regulations? Who is involved in that process and how is the 'benchmark' developed by the Legal Department – where do they get their information from?	This review should be part of the annual process and form part of a Board report. To work efficiently, there should be a good dialogue between the Legal or Compliance team and the business so that change can be captured and reviewed. This can be perceived as adding another layer of administration, but the consequences are so serious that making sure everyone knows what their obligations are for managing security risk is not an option. The size of the gap between what is happening, and what should be happening to ensure compliance will dictate how much needs to spent in closing the gap.
Is the corporate standard for security risk management enforced and verified by an assurance process such as audit or a risk review?	Setting the standard is important, but non-compliance with the same could lead to higher sanctions and fines as well as loss of confidence by stakeholders. The occurrence of a security risk where own policies were not followed can also be detrimental to the appraisal value of the company reflected in its share price. The same affect could be extended to authorities, which could levy sanctions and fines for non-compliance.
Is the Legal department involved in the disclosure statement preparation and are they familiar with security risk scenarios and threats?	The declaration of unmitigated security threats and risks should be declared in public disclosure statements to ensure safe harbour from investor lawsuits from losses occurring from the same.
What is the dialogue like with regulators and authorities on security risk, developed scenarios etc?	Regulators and authorities have a responsibility to ensure the continued integrity and security around energy infrastructure assets. A shared understanding of threat scenarios and mitigation measures can reduce any difference of view on what constitutes an appropriate response. This is important in countries where the authorities can compel a company to invest in measures it may not agree with.
For new projects, what security risk assessment is required as part of the issuance of local permits and permissions? Is the Legal department responsible for ensuring compliance or is it the Project team?	This will vary, but are influential on what a company can and cannot do. The authorities will make an assessment of what is permissible based on a risk assessment to the local area and community and they may require a security plan to be prepared and monitored. They may also be required to commit security personnel, emergency services, police response by the Company and the costs of these services will be recovered from the Company via various means.
Are any of the Company's assets classified as 'Critical' on criteria applied at National level or at European level (as defined by the process set out in the European Programme for Critical Infrastructure Protection)?	The implications of this vary from country to country and the Company must be aware of how the authorities regard the criticality of their assets, whether in the home or host countries. As noted above, this could require an additional investment in security measures to satisfy requirements driven by concerns outside the Company's own sphere of interest. This highlights the quasi-public sector role critical assets play in ensuring economic resilience and the security of supply.

5.3 Strategy

Strategy is the single most important influence on the security exposure of a Company as it relates to opportunities to create shareholder value.

It can also cover the disposal or re-structuring of existing activities, but this too is with the objective of creating shareholder value and such initiatives would always be part of an overall growth strategy. The following diagram is by McKinsey & Co and shows the various means by which this can occur, with increasing risk associated with each strategic option that could be commercial, operational, financial or security related.

Fig. 5.3.1 McKinsey Growth Strategy



The growth strategies selected by the Board of Directors do generate risk and the balance between that risk and potential reward is debated and approved at that level. However, the extent to which that debate includes a comprehensive review of the security risks involved varies a great deal from company to company.

Many energy companies do not have a Security Strategy document and an integrated risk management framework to implement one, but the financial implications are there nonetheless, as is the risk.

The identification and quantification of corporate risks, and strategies for their effective management and mitigation, are becoming required formal statements in corporate announcements in the wake of existing and forthcoming legislation in the US, Europe and elsewhere. Given the potential impact of security events to disrupt and delay and damage reputation and activity – security risk falls within the scope of this requirement.

There are several aspects of strategic planning which touch on security and these are horizon scanning, opportunities and threat analysis and competitive positioning. The outcomes from each activity reflect implicit decisions about a Company's tolerance for security exposure across the activities it wishes to grow or develop.

AREA OF IMPACT:
STRATEGY

5.3.1 Horizon Scanning

Visibility

Low	Medium	High
		X

Performance

The analysis and monitoring that is captured under this activity would demonstrate the inclusion of security threats. A Company may have a regular risk report noting the risk environment, possibly relating to political and economic variables in particular regions or countries. Security should be a key element of such a report. So, if the analysis is comprehensive, security threats are being monitored and reported upon in a manner appropriate to the Company's risk tolerance and strategy.

Definition & Comment

Monitoring changes in a Company's environment is a key aspect of strategic planning and this should include changes in the threat environment as well. How a Company undertakes this activity, by whom and where, will influence the cost and effectiveness of the process. Security threats create barriers to growth by deterring investment and reducing a business's willingness to take risks. They can also increase transaction costs.

Financial Drivers	Impact & Implications
Who is responsible for monitoring the threat environment at regional, national and local level? This might be a shared responsibility or clearly delineated between the Strategy team, the Risk department and the business.	What is the process for discussing changes in that environment that might influence the agreed strategy or financials?
Does the Strategy team know what the Board's tolerance for security exposure is and, if so, how is this taken account of in the strategic evaluation process? Is there a Scenario Planning process in the Company and does it look at risk outcomes and consequences? Who is involved with this and have they got the right experience?	If this is unclear, then the tolerance level has to be derived through an iterative process which is time-consuming and inefficient. Using scenarios to identify and consider alternative options and their consequences draws on expertise in the business into a comprehensive process that can look at all variables and make informed recommendations to the Board. This is a key tool that can be used to get a shared understanding on risk tolerance and how that can be managed through alternative strategies.
Who is responsible for gathering information on the threat environment?	Reliable information can be hard to obtain. Does the Company use its own sources or buy it, if so, from whom and how much reliance is placed on it?

AREA OF IMPACT:
STRATEGY

5.3.2 Opportunities & Threats

Visibility

Low	Medium	High
		X

Performance

Similar to 3.1 it will be evident in the discussion about strategies how well the security risks to those strategies have been taken account of. Obtaining the "sign-off" of the Security Director or Manager does not mean that information about security threats has been **understood by those responsible for monitoring opportunities and threats** and developing strategy as a result. The analysis and recommended outcome must reflect that knowledge.

Definition & Comment

Risk tolerance, market knowledge, market expectations all inform the opportunities a Company has to create value and the threats to that value. The process used to select and evaluate opportunities varies, but it will include a consideration of the risk:reward balance between each one.

Financial Drivers	Impact & Implications
At what point in the decision-making process do security threats feature as part of the discussion about options?	Depending on risk tolerance (which may not be defined precisely) security threats can rule options in or out. For example, persistent loss of revenue from organised crime can erode confidence in earnings even if still value creating. Engagement with a partner whose track record or country of origin might raise ethical concerns could close off a financially attractive option. Security threats can be derived not just from a Company's activities, but from those of others it has a dependency on. So understanding the vulnerabilities of each strategic option is a critical part of making the right choices.
Has there ever been an incidence of a security threat putting on hold an operational activity or prevented a plan being fulfilled?	Under such circumstances the Company's BCP process would come into operation. Decisions about business resumption or changing strategy and informing stakeholders of those decisions needs to be managed. Getting this wrong can be costly.
What is the process of responding to security concerns/threats that emerge after strategies have been approved?	Security risks and threats can emerge quickly so the process for reporting them needs to work efficiently - how joined up is the process?

AREA OF IMPACT:
STRATEGY

5.3.3 Competitive Positioning

Visibility

Low	Medium	High
		X

Performance

As with 5.3.1 and 5.3.2 discussions about competitive positioning will be evident in the strategic planning process and the operational models recommended for undertaking particular strategies. Decisions about security risk tolerance should reflect the judgment of the Board of Directors, but knowing how competitors manage security threats is an important consideration. This knowledge should also be evident in partnering decisions (see 5.7).

Definition & Comment

Competitive positioning reflects strategic thinking about opportunities and how to grow profitably and create shareholder value. In the energy sector, there is often a good deal of collaboration between players and this is evident especially when there is a security event or incident affecting players in a particular locality. However, there is competition between companies in each part of the energy value chain, and how each Company views potential security threats to its own assets may be influenced positively and negatively by competitor behaviour.

Financial Drivers	Impact & Implications
To what extent is there collaboration between the Company and its competitors around particular assets or in a locality?	Such collaboration can result in a sharing of risk arrangements and the cost associated with delivery whether pre or post an event. This might relate to community relations, evacuation planning, government negotiations.
How would you compare your security risk appetite with those of your peers? How would they describe your positioning in relation to security risk?	In relation to partnering, most companies look for partners with a like-minded approach to key areas such as risk. No Company wants to be implicated, tied up or having to explain a position it would not usually adopt, because of its partner organisation. There is a clear reputational risk of doing so.
Do peers take riskier decisions that have allowed them to grow value in areas that have higher risk adjusted returns?	Risk tolerance acts as a brake on opportunities that can be value creating for those with a different perspective of how that risk affects their Assets.

5.4 Risk Evaluation

The global risk environment is dynamic with natural disasters, terrorism, political risks, economic uncertainty, civil disobedience and war, increased regulation and financial volatility challenging all players.

The energy industry is particularly exposed given the global nature of its activities and contribution to global and national economic resilience. So the challenge exists to monitor change, identify emerging risks, eliminate existing threats before exposures occur and re-evaluate the range of potential consequences.

Earlier the importance of developing **all-risks scenarios at a corporate level** was raised as a means of keeping existing risk frameworks current and alive to change. These, along with clarity about the risk tolerance of the Board for specific risk outcomes, will influence the level of risk management in place.

In the energy sector, at an Asset and site level, Health, Safety and Environmental (HSE) and Operational (people, process, systems) risks are crucial, so the focus of this subsection is to pose a set of questions to establish how both areas of risk influence expenditure on security risk management. It also includes a section on compliance or audit.

As noted in 5.1 on Market Expectations, there are external stakeholders with a keen interest in the **overall level of risk** in an organisation they are investing in, rating or funding in some form. They want to know if that level of risk will allow returns to be generated that create the level of shareholder returns investors and the market want to see, whether creditworthiness will be impaired and whether covenants will be breached.

Insurance companies also have a keen interest in risk and would want to know in some detail about how risk scenarios are developed and acted upon. (Insurance interests are covered in 5.5 on Finance).

Ultimately, however, the group of individuals most interested in the risk profile of a business is the **Board of Directors**, who are accountable for the impact of that profile on shareholders and regulators.

AREA OF IMPACT:
RISK EVALUATION

5.4.1 Health, Safety & Environmental Risks (HSE)

Visibility

Low	Medium	High
		X

Performance

Given the monitoring and reporting infrastructure already embedded in HSE management, where security risk is part of that department, **it should be visible on that infrastructure**. If not, the question should be asked how the head of the HSE department knows if security risks are being identified, evaluated, monitored and reported on?

Definition & Comment

For many energy companies security risk management is part of the HSE department. This is a positive if security risk has visibility and has a remit that extends beyond the boundaries of the HSE department, but this is rarely the case. In some energy companies, there are completely separate risk management processes in place for security even within the same department which reinforces a lack of awareness and encourages a 'silo' approach to risks that should be looked at together. Indeed whilst HSE risks are often site-specific, the causes and consequences of security risks are broader for several reasons:

- They are driven by external events
- They are complex and multi-faceted
- They have serious and long term consequences.

If security is part of the HSE department in the Company concerned, the questions here are designed to establish how visible and supported security risk management is as part of that department. If not, it is likely that the team responsible for security risk management is under-funded, over-stretched and lacks profile in the business.

Financial Drivers	Impact & Implications
Is the HSE Department of the Company responsible for security and, if so, how visible/prioritised is it?	How is security defined in the company and how is it resourced and managed? Does the HSE Department have the right skills to manage security risk? Is security part of the HSE budget?
What percentage of HSE incidents are caused by security breaches?	HSE incidents can be caused directly or indirectly as a consequence of an exposure or failure in security. Identifying the underlying cause is important, so that the correct remedial action can be put in place, including communication and preventative measures.
Is there a relationship between the HSE and Risk Management function? Is there a relationship with the peer group?	If there is any relationship, how do they influence, and what do they expect from, each other?
Does the HSE Department of the company have the knowhow of security management? Are people equipped and supported to manage risk well?	Does the HSE department have a good understanding of the cause, impact and preventative measures related to security risk? This will have an impact on the remedial actions, communication channels and preventative measures put in place.

AREA OF IMPACT:
RISK EVALUATION

5.4.2 Operational Risk

Visibility

Low	Medium	High
	X	

Definition & Comment

Operational risk is the risk of financial losses resulting from inadequate or failed internal processes, people and systems from external events. Such events might be security related and can disrupt processes, people and systems (Note that Systems are looked at under 5.8). The robustness of operational risk management will mitigate security risk if done properly, and this is what the questions are designed to find out.

Financial Drivers	Impact & Implications
How is operational risk managed within the Company at the moment and does it include security risk?	If this is an area of risk that is visible and where there is clear management accountability, it is likely that there will be strong links with security.
When incidents occur that disrupt operations, BCP plans etc will become 'live' to deal with that disruption. To what extent are the causes of that disruption shared around all risk practitioners in the Company to a) make sure they are understood; b) ensure any linkages are identified; and c) to capture any learning?	This will aid understanding about the causes and consequences of risk events on the business and promote an inclusion of security threats into the overall understanding of risk. As with Scenario Planning, the more inclusive the approach to risk is, the more robust the measures will be to manage it.
Have any measures been introduced to strengthen operational risk and what have the benefits been? Who was involved in identifying what measures might be required?	Any investment in strengthening operational risk could benefit security risk and so it would be cost effective to make sure this included security where possible. It might be the case that a review of procedures for security purposes might also benefit operational risk considerations, such is the overlap between the two in terms of practical mitigation measures relating to people and process.

AREA OF IMPACT:
RISK EVALUATION

5.4.3 Compliance & Risk Assurance

Visibility

Low	Medium	High
	X	

Performance

Any process designed to deliver assurance about compliance will set out how what it is looking for and how the review will be done. So any gaps in relation to security should be clear. If it is covered then it will be commented upon by the compliance or internal audit team.

Definition & Comment

Compliance and Risk Assurance give an objective view on whether risks are being managed to a level expected by the Board of Directors and Executive Management. A Company might have a compliance department, but usually in energy companies it is Internal Audit who undertake the compliance and risk assurance function. The cost of compliance is usually recharged to the business being reviewed and its focus can increase or decrease, depending on the perceived 'riskiness' of the activities. Risk Assurance is a priority area and many energy companies are making compliance a focus of attention in the wake of concerns over HSE or security.

Financial Drivers	Impact & Implications
Is there a formal security risk policy in place and how is it monitored?	Having a formal security risk policy ensures both awareness and resourcing of the same. Inclusion in a Business Continuity Plan and relevant risk reports ensures awareness and responsibility. Top management being aware also ensures support for security programmes and a security risk aware organisation. As mentioned under 'Governance & Reputation', it is tangible reinforcement of the kind of security culture a company wants to instil.
Does security risk fall within the scope of the Internal Audit or a separate compliance team?	It is important that the compliance/audit team members have the right skills and experience to evaluate whether security risk is being managed well and in line with the corporate policies and expectations.
How broad is the scope of the Audit or Compliance review?	What kind of recommendations are made? Is it clear to all parties what the purpose and scope of the Audit or Compliance review is?
What processes have the security team had to put in place to meet compliance requirements?	It is important to identify the existing processes in the security department and to see whether additional processes had to be put in place (e.g. having to create documentation, KPIs, providing and audit trail of decisions, etc.)

5.5 Finance

The focus of the Guidelines is to identify the financial implications of a Security Strategy, so they are written essentially as a guide for the Finance Director to use to identify what that financial implication is across the business.

However, **finance itself can drive the financial impact of a Security Strategy** simply because it is an inherent part of the decision-making in every part of the business. The Finance Director and their team are responsible for making sure that financial controls are in place to maximise the profitability of each part of the business in line with the Corporate Strategy; and for the regular financial reporting that monitors how well the business is performing in line with that Strategy.

The financial interests of external stakeholders were considered in Market Expectations so in this subsection, finance encompasses **those areas within the control of the Finance Department** that can influence the expenditure on managing security. So it includes choices about insurance, investment appraisal, financial management, performance and pricing.

AREA OF IMPACT:
FINANCE

5.5.1 Insurance

Visibility

Low	Medium	High
		X

Performance

Risk assessment is fundamental to the insurance process so it should be evident whether or not security risks have been taken account of by insurers or the captive with a clear link to the cost of insurance. If the answers to the questions are inconclusive or vague, then there are reasonable grounds to doubt the inclusion of security risk. Where there are tax advantages to be gained by a demonstrable investment in risk mitigation measures by a Captive this would be known to the Finance Department.

Definition & Comment

Whether a company self-insures or goes to the market for insurance, the risk still has to be known, and disclosed. For some risks, the price is commoditised, but for large assets and projects, that is unlikely with an insurance company keen to understand the risks and price the right package for the client. For the Guidelines, it is important for a Company to know the cost of insuring ALL security risks, whether and however that insurance is sourced and funded.

The questions are broad and intended to provide a guide for further investigation across all areas where insurance is bought, for example, by the Personnel department and business teams.

A typical risk assesment process is set out in Box 5.5.1.

Financial Drivers	Impact & Implications
Who is responsible for overseeing the insurance process in the Company?	How widespread is the delegated authority to source and supply insurance cover to the Company? Does this responsibility reside with the Finance Department?
What risk assessment process is used to identify and evaluate security risks for insurance purposes? How often is that process applied and insurance arrangements reviewed?	To obtain the best pricing from perhaps a pool of insurers, it is important to have a visible and consistent process for risk identification and evaluation. Insurers will have their own process, how different is it from that used by the Company and how does that influence the premiums quoted as a result of its application?
Is the level of self-insurance for deductibles understood by management? Are exclusions well understood? Are there any special security risks related exclusions other than what is customary, i.e. war?	It is important that insurance coverage is well understood. Management should be aware of any key coverages that are excluded especially if related to security risks. In some locations losses to P & E related to security risks such as civil disobedience, civil riots etc are reduced or removed. i.e. Arab Spring. Such gaps need to be understood. Any specific non-customary exclusion related to security risks should be highlighted.
Is there is a list of uninsurable security related events and are the potential losses from an occurrence understood by the Executive Management team?	Certain security related risk may not be insurable. These insurance gaps need to be understood and thought of when thinking of a risk tolerance for the same as well as the Company's overall tolerance.
Is there a link between the security threat and other threat scenarios into the insurance solicitation/ evaluation process?	This is a useful means of ensuring coverage as well as apportioning costs to some security risks.
Is a Captive used and if so, why?	There are financial advantages to using captives, but the benefits need to outweigh the disadvantages. What does the Captive cover and how often is that reviewed? Often management of the Captive falls within the Finance department, what process is used to review the threat environment and changes to the security risk profile for those assets falling within the remit of the Captive?

Box 5.5.1

The risk assessment approach on a large energy project starts with a Front End Engineering Design (FEED). Basic risks will be identified and listed, this qualitative approach allows new risks to be added as they are identified with the progress of the design. In energy projects the key issues are normally around the product and the product inventory. This is where the quantative (QRA) work starts. Acceptable risk levels are applied and the design modified in an iterative process until the risks are either under the allowable values or are ALARP (As Low As Reasonably Practicable). QRA risk is normally expressed in terms of events over a period of time, e.g. 6E x 10-^{6}Y (6 events in a million years). The impact of the event will be quantified, loss of life, financial etc. RAs and QRAs are used by the authorities for planning approval purposes and subsequently in the HSE for regulation, e.g. COMAH Safety Cases.

The major risks will then put on the risk sheet by the broker. The risks are reviewed regularly and particularly after an event, ie 9/1, insurance premiums rocketed for a while and then eased back once the event and risk were better understood, likewise Piper Alpha.

Security threats may follow the same process as all other risks but would tend to be more “live” in that events have been more common in recent years. Security risk should be on the Risk Register, so it is reviewed, whereas the safety risks inherent in the plant operation are more static, build it to the right design, operate it correctly, maintain it well and the risks won’t change very much over time.

With operations in the energy sector, insurance will only cover a very small part of the risk, consequential loss can never be covered. The insurance normally covers the cost of returning the operation to the condition it was in prior to the event. It is unlikely that a Company would insure against loss of income. Indeed many large energy companies have their own Captive insurance company where the same rigour should be applied to risk identification and quantification, so that the Board has assurance the right decisions are made both for financial and risk assurance reasons.

AREA OF IMPACT:
FINANCE

5.5.2 Investment Appraisal

Visibility

Low	Medium	High
	X	

Performance

For every project the Company is investing in, there is likely to be a security component. What that component is supposed to do and achieve should be clear in the investment appraisal process. What is the security requirement, what is that based on, what risk reduction needs to be achieved, how is that possible and what are the options? All these questions should be clearly set out by the team proposing the investment with specific performance expectations defined that can be tracked throughout the Contract. (See Phase B and C of PRISM® for an explanation of what should be expected here).

Definition & Comment

One of the most visible areas of financial expenditure on security risk will be on new assets or developments that have been approved as strategic growth opportunities for a company. Current practise for most infrastructure projects involves a competitive tendering process for a Scope of Works to be delivered by an Engineering, Procurement and Construction (EPC) company, who sub-contract as and when required. **What is not often clear is how the security requirements for the project are identified, incorporated into the tendering process, evaluated and approved.**

As a result, it is not unusual to find that the work required to deliver an unspecified level of risk mitigation is either swept up under part of the contract that might, for example, relate to HSE; or dealt with past the point at which security design features can be incorporated efficiently; and/or are bolted on at the end where it is unlikely they will deliver the level of risk mitigation expected, but perhaps not articulated, by the Contracting party. The potential for contract variations and cost over-runs is clear.

In addition to this and because of how Contracts are managed within an energy company, on a project by project basis, working with one dedicated security integrator and getting the financial benefits across multiple projects that could be obtained as a result – **does not happen**. Instead the security element remains 'hidden' with value for money hard to identify and even harder to prove. **A more strategic approach to sourcing and delivering security systems for enhancements or new projects is to be encouraged.**

The questions are focused on the investment appraisal process and are linked to those on Asset Management especially with regard to the concept of Value for Money (VFM). This is relevant to the Investment Appraisal process as in some regulated sub-sectors, it supports a mechanism whereby compensation can be payable via the tariff to the operator once VFM has been established by an approved auditor. However, whether this is available to the operator or not, the concept of ensuring VFM should be a priority for any company and a commercial Performance Audit provides this assurance. (The VFM process is set out in 5.9).

Financial Drivers	Impact & Implications
How is security risk incorporated into the Contracting and Tendering process for new infrastructure projects? Who is responsible for ensuring that such a process, if it exists, is applied?	Identifying the risks to a project and ensuring that these are addressed is fundamental to any investment appraisal project. Security threats and risks should have been identified before the investment appraisal process was completed as that process is designed to confirm financial returns and sensitivities to those returns. The probability of disruption to those returns may or may not be quantifiable, but should have been identified, not least because of insurance considerations.
How does consideration of security risk at this stage move into the Contracting process as a set of specific performance-led design requirements to provide the assurance required by the Company and others involved in funding the investment that security measures will deliver?	Unless security considerations are taken account of at the earliest stages it is unlikely that defined performance standards will be incorporated into the Tendering process for an EPC player or HSE consultancy.
Does security risk play a role in setting hurdle return rates for new investments? Does the Company use any other measure for ROI apart from ROC, for example, a risk-adjusted return? If so, what risks are measured?	This would provide evidence that this area of risk had been identified and evaluated in sufficient detail to support a decision about risk pricing. (The use of risk-adjusted returns for ROC measures may be unusual in the sector, but is something to be encouraged as the data will exist and the concept is well developed. It also focuses attention on key decisions about pricing and cost of funds.)
Are assurances sought by the Company about the level of performance and risk mitigation delivered by security measures, once these have been implemented by the Contractor?	Without such assurances, the Company will not know whether the security around its investment is going to deliver the risk mitigation required and whether the money spent has achieved its objectives.

AREA OF IMPACT:
FINANCE Cont.

Is there a review after the investment has been signed-off to assess how well security risks have been addressed and whether or not the process to do so has been effective?	As noted above, current practice would suggest this is not done well, resulting in variations, unforeseen costs and compromises. A performance audit of the security risk investment would identify whether the Company has a) approached the management of security in the most efficient manner; and b) achieved value for money (VFM).
How broad in scope is the Quality Assurance (QA) process used by the Company?	A good QA process is a pre-cursor for a VFM or performance audit. When applied to the security risk elements in an infrastructure build it can provide assurance that the expenditure proposed will deliver a level of security that a) delivers a defined level of risk mitigation; b) is 'right first time'; and c) works. The Capex costs of physical and procedural security can be high and the QA process needs to be embedded into the project management process. (Note that it is only recently that QA has been applied to security programmes and not many energy companies can prove that it is in place for this aspect of expenditure.)

AREA OF IMPACT:
FINANCE

5.5.3 Financial Management

Visibility

Low	Medium	High
		X

Performance

The processes themselves would be written in such a way to include security-related expenditure – how that is described and captured so that an aggregate amount can be consolidated will vary from company to company but the principle remains – any expenditure planned for the forthcoming financial year or that arises during the year should be noted and justified as part of the budget process. Similarly with cost management any cost reduction measures will have been agreed in advance and the consequences of them identified.

Definition & Comment

Financial Management in this context refers to budgets, projections and cost management – two key processes that should capture any expenditure on security-related initiative in any part of a Company.

Financial Drivers	Impact & Implications
How is the cost of security risk management captured in the budgetary process for each department? How are changes to those budgets to respond to an emerging security situation reviewed and approved?	For those areas shown on the impact assessment each department will need to ensure the cost of its activity to implement the Company's Security Strategy is captured in the budget. How 'visible' that security expenditure is at present will vary, as noted, the obvious areas of expenditure around physical, IT and personnel security should be fully costed, but other areas may not be. Whilst it is quite possible for potential spend to be captured under contingencies, this is not ideal as the cost may be ongoing or recurring or have an impact on other areas of corporate expenditure or activity. For example, a shift in operational activity to a contingent location because of security concerns has an immediate financial impact on the cost of maintaining the teams and activity, even on a limited basis, but this can continue for a long time, it does impact on local CSR activity, supplier contracts, projected returns, communication, investor relations etc.
To what extent do financial projections take account of potential security threats that could cause a delay or disruption to activity? Many Companies use exceptional budgets or contingency funds to deal with any unplanned expenditure, but for ongoing delays, an impact on projections is inevitable and needs to be reported.	There are several stakeholders interested in the financial projections prepared either for a particular investment or the business as a whole. Any change to those projections, regardless of cause, needs to be explained and taken account of in the planning cycle, especially if the cause requires a significant shift in focus. Scale and visibility are key drivers – low level losses from criminal activity may be already taken account of and need not be disclosed unless they increase materially. It depends on the risk appetite of the Company and the extent to which the impact of security risk is identified and discussed. Often, the operational impact is more visible than the financial cost.
To what extent are security measures captured within cost reduction programs driven by local or Head Office requirements?	As long as security risk is regarded as a cost, rather than a business enabler – it will come under scrutiny when companies are looking at areas to reduce cost in. The Finance department may not be interested in the consequences, in particular how risk mitigation is compromised as a result and whether that is acceptable, or not, to Management. How well that is articulated may be down to the security team. Security managers rarely have a budget, often it is part of either facilities management or the HSE budget. So there are often conflicting demands on funds and that is only for areas where security expenditure is visible. For those areas where the need to manage security risk is less visible, the chances of identifying cost is more difficult.

AREA OF IMPACT:
FINANCE

5.5.4 Performance Management

Visibility

Low	Medium	High
		X

Performance

Definition & Comment

Performance management is about tracking results across Key Indicators of Performance (KPIs) before the outcomes hit the numbers. Incorporating security risk can either be indirect; for example, maintaining continuity of production is a consequence of good security management; or it can be monitored more directly on the number of security related incidents. Monitoring performance tells a Board of Directors if its Corporate Strategy is on track, **so reflecting the impact of risk on that strategy is important – the challenge is to find the right measures and accurate data on which to base them**.

The following questions are aimed at understanding how well risk is incorporated into performance management – if this is well developed, then the framework exists for adding security risk onto it. Remember that setting performance standards for security systems for new projects or enhancements as noted under Investment Appraisal are equally valid performance measures.

Financial Drivers	Impact & Implications
Does security risk feature in performance measures used at operational and corporate level?	HSE is a good comparator as there are some good metrics being used to monitor potential and actual incidents. It is possible to develop metrics that do the same for security risk – linking investment to risk mitigation by specifying performance standards for equipment or systems, changes in the threat environment to changes in operational activity, testing and exercising etc.
Are performance standards set in relation to risk mitigation measures?	This might be captured as part of the Investment Appraisal or Contracting process. However, as with any form of expenditure – a Company wants to know if it has got what it paid for. Setting that as a performance measure is the best way of answering that question as it defines the corporate expectation at the outset and provide a benchmark against which the work can be evaluated, and then paid for.

AREA OF IMPACT:
FINANCE

5.5 Pricing

Visibility

Low	Medium	High
		X

Performance

If a Company knows what its security exposure is across all activities – then decisions about how to offset that exposure covers insurance, reserving policy as well as pricing, which might include the potential for compensation via the tariff in some sub-sectors, and the cost of capital. The Finance Director will know what the Company's approach to pricing for risk is and how it applies to security.

Definition & Comment

Pricing risk into the cost of capital, services, insurances and budgets **is as applicable to security risk**, as it is to HSE and operational risk. To do this requires that the Company knows what its risk exposure is and making an informed choice about how to offset its financial impact – just as it does for insurance purposes.

In some regulated sub-sectors the cost of security risk mitigation measures can be recovered via the regulator, subject to VFM checks, but this only applies to one sub-sector, in one country in the EU. One of the issues facing policy makers is the extent to which a level playing field is desirable and possible, but the energy sector is one where there are many converging agendas focused on the pricing of energy to consumers, the security of supply and, within the EU, IEM interests.

If the cost of the risk was de minimis then its impact on pricing would be as well, however, the cost of funding programmes for physical, procedural and personnel security is significant enough for an Asset Owner to think about how to offset that cost. This is an interesting topic that is being discussed amongst policy-makers and will become more important as those converging issues develop.

One further point is the relationship between 'home' and 'host' countries and the extent to which their requirements both for security and pricing vary. For companies operating globally, not only may there be national security related regulatory and legislative requirements to be met, but the potential to offset the costs of compliance will vary and that cost has to be borne somewhere in the business. The question is where?

Financial Drivers	Impact & Implications
To what extent does pricing reflect any risk involved in providing the product or service to the end user?	If the Company does this, then it is possible to apply the process or methodology to security risk – it has a precedent.
Has the Company been involved in discussions with its regulatory authorities about pricing for risk?	This will vary from country to country. As noted earlier, the extent to which regulatory and security services are involved in defining security mitigation standards for a sub-sector will vary.

5.6 People Management

In the energy sector ensuring the safety of people, whether employed as staff or a contractor, is a key priority. Security is as important. The purpose of this section is to outline the considerations that drive the potential expenditure on security by the Personnel or Human Resources (HR) department as a visible cost. It looks at management, recruitment, appraisals, contractors and training.

As with other areas, it is important to understand how the budget process works in relation to expenditure on people – most HR or Personnel departments are 'cost centres' with the business units paying for direct costs and a proportion of the support services provided by those teams. So it is important to identify where responsibility lies for managing the security of people and how decisions by the business impact on the HR teams and vice versa.

Finally, culture also has a significant role to play in how security is promoted in the organisation and defining the behaviours management want to see evidence of in the company.

What performance is expected from security measures needs to relate to business objectives and the specific actions agreed to implement them. If this framework is in place, then measurable outcomes are possible. If it is not, then results will be difficult to identify and the management of the security risk from those working inside the organisation is likely to be fragmented across the organisation and not joined-up.

How an organisation is structured can also have a significant impact on how risk is managed – this is one security threat where 'gaps' can be exploited quite easily with those with an inside knowledge of the business.

Given the profile of 'Personnel Security' Box 5.6.1 provides a definition as a reference for the questions.

Box 5.6.1.

Personnel security is a system of policies and procedures which seek to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes. These purposes can encompass many forms of criminal activity, from minor theft through to terrorism.

So the aim of personnel security is to minimise the risks. It does this by ensuring that organizations employ reliable individuals, minimise the chances of them becoming an insider threat once they have been employed, detect suspicious behavior and resolve security concerns as soon as they have become apparent.

AREA OF IMPACT:
PEOPLE MANAGEMENT

5.6.1 Management Skills

Visibility

Low	Medium	High
	X	

Performance

Measuring the effectiveness of managers in identifying potential personnel security issues has to be a requirement against which a manager is appraised. Is it a requirement that is explicit and discussed amongst managers? Is it included in written down procedures about managing staff, dealing with problems or concerns etc? This provides the performance context for Management Skills as a means of mitigating the risk from people inside the Company.

Definition & Comment

The quality of management is crucial to ensuring the security of people, not only in demonstrating the culture of the Company, but also in knowing the people they are to manage, being able to identify potential problems, anticipate and react to changes that could lead to actions that might undermine the security of the Company, providing an 'open door' policy and getting the balance right between management and being one of the team. Getting this right will, without costing anything, have a more positive impact on reducing potential security risks, than many physical or procedural measures, important as they are.

Financial Drivers	Impact & Implications
What role does the HR/Personnel department play in defining the management skills required in the Company?	It is likely that the department defines the management competencies required at different levels or grades in a Company. How is responsibility for ensuring the security of teams within the Company allocated amongst the management group? Is it a clearly stated requirement or not?
How explicit are the responsibilities of managers in relation to security? Are they as clear as those set in relation to safety? Is there evidence of these skills being applied in the Company?	There are three skills that are particularly effective in reducing the threat of insider activity: • **Awareness**: Understanding why people change, become disillusioned, demotivated. • **Listening and Observing**: Identifying early on what is or could go wrong and why. • **Influencing**: Being able to tackle issues early on, quickly and effectively.
When does the HR/Personnel department become involved in dealing with concerns over a member of staff or a contractor? At what point does the Manager ask for their input?	The point at which a Manager decides to engage the support or advice of the HR/Personnel department may not be written down, but understood within the cultural context of the Company. It is important to know how concerns are managed and who is responsible for dealing with them.

AREA OF IMPACT:
PEOPLE MANAGEMENT

5.6.2 Recruitment & Appraisals

Visibility

Low	Medium	High
	X	

Performance

Identifying how well the security risk from those inside the organisation is being managed through the recruitment and appraisal process is a combination of direct and indirect measures. Direct measures can be derived from screening and the objectives set for it; indirect measures are derived from checklists developed for both areas as well as those in place for Management Skills.

Definition & Comment

How a Company selects new staff and contractors and then monitors their actions and behaviours once in employment are critical points at which security risks can be identified, managed and monitored. The approach used will influence how much or little a Company wants to spend – any controls must be proportionate to the scale and nature of the threats faced, so there needs to be good communication between those responsible for monitoring the threat from insiders and those responsible for managing it.

Any controls must be proportionate to the scale and nature of the threats faced. A full personnel security risk assessment will identify the high priority threat areas and help ensure there is sufficient buy-in both from employee groups and the board. This is what will drive the cost made by a Company to reduce the risk to within acceptable levels.

Financial Drivers	Impact & Implications
Is there a policy on screening? Who decides what kind of screening is appropriate to the threat and the Company? Are all stakeholders who have an interest and responsibility engaged in the screening process?	Screening can fulfil a number of purposes. (i) To identify individuals displaying behaviours that have been seen before in previous insider cases; (ii) to detect actual insider activity; (iii) to assess the role posed by an individual moving to a more sensitive role. See Box 5.6.2. Pre-employment screening and appraisals will be more effective and efficient if they are an integral part of an organisation's policies, practices and procedures for recruiting, hiring and training of staff. So is there input from HR, Security, Legal and business unit managers?
What level of screening is undertaken on new and existing employees and contractors?	The process used to undertake screening can capture a number of different approaches – the extent of which depends on the threat identified by the risk assessment process and the level of screening required. It takes time and has a cost, especially if external checks are involved.
How robust are ongoing personnel security measures and the risk assessment they are based on?	Is the organisation satisfied it is maintaining a 'baseline' standard for pre-employment screening including identity verification, verifying right to work in a particular country (nationality and immigration status), confirming employment history and qualifications, verifying criminal record? Additional levels of security (for instance, if certain staff have a need to access sensitive information on a regular basis or as a result of regulations imposed by national CNI agencies) may result in extra costs. Organisations may be subject to a range of 'insider' threats – disaffected staff, journalists, commercial competitors, single issue groups, terrorists or hostile intelligence services and motivations can be varied including financial gain, coercion, ideological, status or revenge. The financial impacts include physical damage, regulatory fines, loss of assets and information, loss of competitive advantage.
How is all the information gathered together on an individual discussed and agreed upon in the Company? What is the process for doing this? Are there any exceptions, for example, if the candidate comes with a personal recommendation from a senior member of staff? Is the organisation confident of its document and identity verification measures from a practical perspective?	The opportunity for information to be missed, misused or mislaid exists and where there may be attempts made at concealment, this can pose a serious risk to the Company. Ensuring there are clear processes in place to gather, manage and share information at the point of recruitment and thereafter is a key part of risk mitigation. Document verification is an integral part of a pre-employment screening process. Staff responsible for this activity need training, experience and the tools to be able to confirm authenticity of documents presented as identification or as part of the employment selection process. Where in house staff are unavailable to carry out this role, it may be necessary to use external providers for these services.

AREA OF IMPACT:
PEOPLE MANAGEMENT
Cont.

Is the appraisal process followed? How would 'warning signs' be picked up and reported on?	The effectiveness depends on the scope and visibility of the process, is it followed, do staff feel it has an impact on their job and prospects, is there follow-up? All these aspects will demonstrate whether the current process is effective both as a means of gathering changes in individual circumstances and responding to them.
Is there counselling in place for employees?	If so, what remit does it have? Is it regarded as a means of identifying potential issues that might pose a risk to the organisation, or not?
Is there a mechanism in place to allow personnel to report security concerns they may have concerning other members of staff?	It is imperative that any mechanism in place meets legal and any regulatory requirements – this is a complex area and should not be regarded as an easy option for a Company wishing to provide a simple tool to mitigate potential security risks.

Box 5.6.2.

BS 7858 is a the British Standard that specifies a Code of Practice for security screening of individuals and third party individuals to be employed in a security environment by an organisation, prior to their employment. It gives recommendations for the security screening of individuals to be employed in an environment where the security and safety of people, goods or property is of extreme importance. It also applies where such a requirement is in the public interest.

Note: A 2009 amendment was issued to take account of the Private Security Industry Act 2001. The Act requires that any person engaged in licensable activities, as designated in the Act, be licensed in accordance with the Act. It is an offence to engage in licensable conduct when not in possession of the appropriate licence. This edition introduces criminality checks if the activity undertaken is not licensable, requires organizations to combat identity theft and fraud, introduces credit reference checking, and addresses the increasing frequency with which employees change jobs.

AREA OF IMPACT:
PEOPLE MANAGEMENT

5.6.3 Contractors

Visibility

Low	Medium	High
	X	

Performance

Assurance that security procedures for the management of Contractors is in place can only be established by a compliance or internal audit review. As with other areas, objectives need to be set about what the business wants to achieve in this area, actions delegated and responsibilities assigned.

Definition & Comment

The use of contractors is widespread in the energy industry and increasing. The main factors influencing the use of contractors tend to be the number of new projects and their location and cost reduction programmes in the company. Contracts can be renewed or extended to a point where a contractor can accumulate a lot of corporate knowledge, hold positions of trust – really be akin to an employee, but without feeling or being accountable to Company values or the appraisal system – both key risk mitigation tools. Whilst reducing headcount is a cost saving measure, the consequent recruitment of Contractors offsets the cost and can increase the security risks to the Company.

Knowledge about the security related risks associated with Contractors will be well known to the Security Director or Manager. This knowledge should be shared with the HR/Personnel department responsible for ensuring that Company Policy and Procedures are followed. The requirement for Contractors is driven by the business so again, a tripartite discussion needs to take place where the security issues associated with employing Contractors are raised and an approach agreed.

Financial Drivers	Impact & Implications
How has the Company's policy and usage of contractors changed over recent years? What has driven that change and has the impact on the security profile of the Company altered as a result?	Handling an increased number of contractors requires resources to manage the paperwork and any vetting requirements. What is the additional cost of this and where is that cost shown? Timescales for recruiting contractors are often tight so there can be pressure to overlook usual pre-employment checks. Contractors can also work for competitor organisations consecutively or simultaneously.
What role do HR/Personnel play in managing the use of contractors? Is there a procedure in place for handling temporary contract workers, who may require additional security measures such as restricted or supervised access?	Are there processes and procedures in place set by HR/Personnel and is their adherence monitored? How often are they reviewed?

AREA OF IMPACT:
PEOPLE MANAGEMENT

5.6.4 Training

Visibility

Low	Medium	High
		X

Performance

Any training delivered in a Company will have training objectives or learning outcomes associated with it. Any security training program will have the same requirement and so it should be possible to see the extent to which the training has been delivered successfully. Making sure the learning is applied afterwards needs to be followed up and embedded either into the appraisal process or as part of a continual professional development program developed by HR/Personnel.

Definition & Comment

As a means of raising and sustaining awareness, training needs to be undertaken with the support of the security department, HR/Personnel department and business managers.

Security training and education is designed to ensure that every employee, regardless of role within the business, understands his/her personal and collective security responsibilities, is aware of security risks and is availed of information concerning mitigation measures they can take to reduce these risks and improve individual and organisational safety.

Financial Drivers	Impact & Implications
Are staff and contractors given security training? If so, by whom and how frequently? To what extent is this incorporated into the induction process?	Who provides this will influence the cost as will the effort made to ensure its effectiveness? Training needs to be updated and delivered on a regular basis.
To what extent are the key messages from the training captured into internal communications and the materials circulated around the Company?	Training, culture and communication are all woven together to achieve a level of awareness and consequent behaviour that can be considered a tangible risk mitigation measure the results of which can be monitored.

5.7 Operations

How an energy company decides to organise the range of activities that contribute towards the operational management of all its Assets varies from Company to Company.

As well as internal functions that the organisation can more easily control and manage, it is important to note that operational activities encompass services and dependencies (that are often provided by other parties) which fall outside of the Company's immediate control. As a result they may be subject to a host of variations affecting reliability, access and cost.

A Risk Assessment process such as that set out in Phase B of PRISM® focuses on operations and includes a detailed Asset Process Analysis that considers issues that may be relevant to security risks (as opposed to a process safety perspective, which is often the case) such as the identification of related threats, critical points, vulnerabilities and dependencies. **This in turn will facilitate more focused and cost effective mitigation measures**.

For the purposes of the Guidelines, this section is related closely to Asset Management and includes defined areas of operational activity involving logistics, procurement, contract management and partner selection. These are the areas where implementing a Security Strategy has financial implications that need to be identified and quantified.

AREA OF IMPACT:
OPERATIONS

5.7.1 Logistics

Visibility

Low	Medium	High
	X	

Performance

Logistics are so crucial to the operation of an Asset(s) that any disruption has an immediate impact. It is possible to develop Key Performance Indicators (KPIs) that cover operational efficiency and effectiveness and link these to financial outcomes. Again the link to what the business strategy is for that Asset(s) and expected financial returns will dictate what those KPIs should be.

Definition & Comment

The nature of the threat environment drives the security measures required to protect the supply chain around an Asset(s), and the cost associated with doing so. This will be borne by the designated profit centre for that activity.

Financial Drivers	Impact & Implications
To what extent do security threats inform the design of the supply chain for high value assets?	The information available to the team making the decisions and access to the right advice.
Are alternative arrangements in place and have they ever been used (part of BCP)?	The availability of alternatives and the cost of them drives the financial impact here. How much time is spent looking at alternatives, in conjunction with any BCP and crisis management planning?
To what extent are logistics shared with other companies?	Are responsibilities clearly defined, esp with regard to an evacuation or crisis situation? This may seem like a cost saving, but only if the arrangement can work to meet the Company's duty of care responsibilities and not expose it to further security risks.
What level and extent of communication is required to support logistics?	Again, varies in relation to environment, but security experience and good contacts with local suppliers and other operators is crucial.
In cases where key logistics or suppliers are critical to the operation of the Company and exposed to similar security risks, are their BCP plans reviewed for the same and coordinated with own plans and alternatives looked into?	Outsourcing, just in time inventory, effective logistics management all are essential cost management factors in the industry. There needs to be consideration of security risks and exposure from the same in decision-making. In case of critical supply chain, one can require looking into the BCPs of the suppliers or alternates. Even if this is not possible it is important to review suppliers and other operators regularly and have the experience to understand how change can jeopardise relationships and arrangements that were previously believed to be robust.

AREA OF IMPACT:
OPERATIONS

5.7.2 Procurement

Visibility

Low	Medium	High
	X	

Performance

With sign-off required by Procurement on all items of expenditure, there should be a mechanism in place to identify security spend. How effective that mechanism is in relation to a change in circumstances where additional expenditure is required needs to be tested. This should relate back to the budgetary process and how any contingency or exceptional spend is managed. This will again vary from company to company.

Definition & Comment

The procurement function is a vital part of financial control and ensures that expenditure meets procurement procedures. Obtaining exceptional and rapid approval for unexpected items of expenditure that might be required in response to a change in environment is difficult to achieve without the right level of support, sometimes from Head Office. So understanding the procurement process and making sure requests are compliant is a key competency for on the ground operations.

Often there will be a procurement manager in a regional or national location who is a key contact for the Security Manager, who, as noted before, rarely owns a budget, but should have the support of the local management team for any requests to spend money on security measures whether in the Security Plan or not.

Financial Drivers	Impact & Implications
What requirements do procurement impose on security expenditure? Does this influence what the security manager requests?	This will be driven by the centre so it should be possible to find out how many requests are approved or not. Getting a feel for how the relationship works between procurement and the security manager would be useful and the role of the local management in endorsing requests for security expenditure.
What arrangements have been made for the planning and procurement of long lead items (LLI)?	Following the identification of Critical Points around a site, procurement of LLIs should be identified and measured. Lack of LLI will have a significant impact on production, and revenue.

AREA OF IMPACT:
OPERATIONS

5.7.3 Partner Selection and Contracts

Visibility

Low	Medium	High
	X	

Performance

The standards a Company sets in relation to its partner relationships (suppliers/contractors) need to be visible and consistent so that a due diligence process can be undertaken with similar results. This is of particular value when benchmarking global relationships, but even with local partners, standards need to be set and monitored and subject to regular review.

Definition & Comment

Increasingly, operations depend on collaboration and good working relationships with partners (suppliers/contractors). Security issues can determine whether or not the home country of the partner faces sanctions or is not regarded favourably by the Company's home country and regulator, to whether the approach to HSSE management is to a high enough standard, what the culture is like and the nature of that partner's other relationships – all can pose a reputational risk to the Company.

The Contracts entered into by the Company with partners will have standard T&Cs that should define clearly how security risks should be managed by partner organisations. It is crucial to remember that a **Company retains the ownership of the security risk** incurred as a result of the activities undertaken by the partner and also from the partner itself.

Financial Drivers	Impact & Implications
Is the responsibility for managing security risk set out clearly in relevant Contracts? Have any contracts been cancelled because of force majeure? Does security risk management form part of any Service Level Agreement (SLA) with the partner?	Reviewing the Contracts required to support a facility needs to be done regularly and must reflect the environment that the supply chain operates within. In higher risk environments, where reliance is placed on national companies as joint-venture partners, clarity over who is responsible for what is a crucial part of managing the Company's own legal risk. What those arrangements are, will drive the costs associated with delivering a specified level of protection in that environment.
Are security checks undertaken on partners?	This should form part of the due diligence process prior to a Contractual relationship being entered into. A Company might decide to proceed with a partner about whom they have security concerns, but this HAS to be raised with the Group's Legal Department so that the right approvals are given. Such checks need to be made on a regular basis, especially when management change, or the environment.
Is there a standard security norm set up for partner selection process?	A common standard for Partner criteria could help place appropriate rigor in the process. It also sets a certain standard of care and forces attention to outliers.
Has any partner been turned down on security grounds?	If so, at what point in the process? How hard has it been to replace a partner? Has the Company ever been in the position of having to choose a partner to pursue a particular strategy which they might otherwise not do?
How are contracts for Contractor's managed? (related to 5.6 on People Management)	Getting the contracts reviewed and updated is the job of the legal department in conjunction with the HR department, but should include the right to audit a contractor's work in progress, disclosure about other work they are undertaking and for whom, and, any standard of behaviour required should be part of the contractual agreement such as use of the internet and email, obligations towards data protection, safety and security awareness etc. This is an additional cost, but is a key countermeasure that must be applied on appointment and renewal of a contract.
Are security checks undertaken on suppliers? How extensive are these?	The security risk assessment should identify dependencies and their criticality to the operation. A Company must undertake its own due diligence.
Are dependencies identified and captured in the risk assessment process?	This is relevant for BCP purposes, but also because of a need to understand the risk exposure a Company has to a third party.

5.8 Systems

From a security risk perspective, the importance of the systems a Company uses to manage its activities cannot be understated. This is a broad topic and it is likely that most energy companies have a team dedicated to Information Security which will liaise closely with the Security team. The Guidelines focus on the financial implications of implementing a Security Strategy in relation to Process Control Systems (PCS) and Information Security.

The protection of PCS is an area often overlooked in a lot of energy companies and yet it is the area most susceptible to security risks. **Traditionally, these systems have been closed and so difficult to penetrate; more recently with the integration of business operation platforms, vulnerabilities have been exposed that require more detailed management**. Information security presents a wide spectrum of challenges to companies seeking to retain material ownership, protect business data and prevent hostile groups from targeting their activities.

The financial, operational and reputational implications of a successful compromise of systems can be significant. These implications can be exacerbated given the media interest that cyber-crime now attracts and the seriousness with which cyber-attacks are taken by governments.

Examples such as the Stuxnet virus targeted at SCADA systems shows the complexity of cyber attacks and the immediate and long-term disruption as a consequence. The emerging phenomenon of environmental 'hacktivism' which includes targeting of oil and gas companies also shows that energy companies need to increase their protection against sabotage, espionage and intellectual property theft. The resulting economic cost and security implications make computer crime one of the greatest threats faced by organisations and their systems. Highlights from the US Office of the National Counterintelligence Executive paper of October 2011 are noted in Box 5.8.1.

Box 5.8.1.

The US Office of the National Counterintelligence Executive published a paper in October 2011 concerning foreign collection and espionage efforts. Although centred on economic and industrial espionage, the report highlights some wider issues:

- China and Russia identified as persistent and sophisticated collectors on a wide range of targets and subject matter.
- Development of an Iranian 'Cyber Army', a domestic hacker group with links to the Iranian Government and reportedly overseen by the Revolutionary Guard.
- Attacks by Foreign Intelligence Services, political and social activists, disgruntled employees, private citizens and criminals.
- Rise of the 'Advanced Persistent Threat' where the target remains unaware of the attack.

Other reporting has expressed concern that there will be an escalation of cyber attacks on industries world-wide with possible targets including power plants, pipelines and petroleum facilities.

The cause of security breaches is usually a mix of people, process and technology – what is described in section 4 as 'Operational Risk'. When looking at the potential threat and causes of incidents relating to compromise of PCS, there needs to be a top-down review of how those factors have created a breach. Given that Process Control and IT Security link many critical components, the management of security risk can fall into two areas.

The first is with the Security Manager who needs to ensure that systems and procedures provide the correct levels of assurance that access to the PCS is sufficient.

The second lies with the IT Security Manager who understands the protection afforded to the system by the Security Manager and is able to implement appropriate layers within the IT system itself. It is a partnership that will require an ongoing dialogue and exercising to ensure that resilience required by the business to perform its operational function gives the required level of assurance.

Box 5.8.2 highlights the key conclusions from the **UK's 2012 Information Security Breaches Survey** and it reinforces some of the observations made in the Introduction about visibility, priorities, lack of investment and awareness. This is despite the very high profile given to Information Security and Cyber-attacks.

If this is the case for this aspect of security risk, one can appreciate why challenging traditional perceptions of security risk and its management is so important, especially where integral energy flows depend on a functioning and secure energy infrastructure supply chain which not only includes physical infrastructure, but also human capital and virtual networks that support the functions of energy systems and operations. **Not investing in security is a false economy**, a point made by the Survey Authors.

Note: Words put in bold by Study authors

Box 5.8.2. 2012 Information Security Breaches Survey

This survey is published every two years and in 2012 447 UK businesses were surveyed by PwC and Infosecurity Europe. The poll is supported by the UK Government's Department for Business, Innovation and Skills. One-fifth of those surveyed are public sector organisations.

Apart from hacking, companies are experiencing many data-protection breaches. The vast majority of firms polled (93 per cent of large organisations and 76 per cent of small businesses) experienced a security breach in the last 12 months: the most serious breaches **generally resulted from failings in a combination of people, process and technology**.

On average, each large organisation suffered 54 significant digital assaults in that 12-month period, twice the level in 2010, while 15 per cent – one in seven – had their networks successfully penetrated by unauthorised parties.

The average cost of a major security breach at a big business last year was £110k to £250k ($177k to $403k), a figure that drops to £15k to £30k ($24k to $48k) for small businesses. SMEs were less frequently targeted with an average of one assault a month.

Despite the prolonged economic slowdown, most organisations are spending more on security. On average, companies spent eight per cent of their IT budget on infosec, and those that suffered a very serious breach spent on average 6.5 per cent of their IT budget on security.

By contrast, 12 per cent of bosses **gave a low priority to security,** with **one in five spending less than 1 per cent of their IT budget on information security – possibly as a result of not being able to quantify and measure the business benefits from spending cash on defences**.

PwC note that organisations which suffered a very serious breach during the year spent slightly below the overall average on security. **The key challenge is to evaluate and communicate the business benefits from investing in security controls. Otherwise, organisations end up paying more overall**. The cost of dealing with breaches and the knee-jerk responses afterwards usually outweigh the cost of prevention.

The UK's Universities and science minister, Mr David Willetts, whose responsibilities include cyber-security issues, commented that firms' reluctance to reveal breaches could later turn out to be embarrassing for them, **noting that a majority of security breaches, particularly in large organisations, originated from insiders**.

AREA OF IMPACT:
SYSTEMS

5.8.1 Process Control Systems (PCS)

Visibility

Low	Medium	High
	X	

Performance

Process Control Systems can be risk assessed with threats identified, vulnerabilities found and measures recommended which will include specific performance requirements. With these in place, it is then possible to link Key Performance Indicators to outputs whether the result of physical, procedural or personnel related actions and processes.

Definition & Comment

The term PCS includes everything that involves Process Control Systems, including systems for Supervisory Control and Data Acquisition (SCADA), process control networks, Programmable Logic Controller (PLC) systems and their physical and organisational environments. Process Automation (PA) environments are complex, and dependencies are increasing because of the increasing level of automation in the PCS. PCS's form the heart of the production process of energy companies which makes them very vulnerable to attacks.

Financial Drivers	Impact & Implications
Are PCS and Information Security considered as an integral part of the security design phase for infrastructure modifications, upgrades or new builds and are they included in threat, vulnerability and consequence assessments?	A Stakeholder Analysis should identify those within the business who have an interest and therefore an input on this subject. When viewing PCS and Information Security in the context of physical security the core components of Detection, Delay, Response and Resilience must be deployed in line with the Information Security Risk owner within the business.
How extensive are the measures in place to protect Process Control Systems? Is there an active monitoring and configuration management in place to maintain an up-to-date inventory of devices and software connected to the enterprise network, including servers, workstations, laptops, mobile, and remote devices?	Access Management and awareness is critical. All persons with authorised access to process systems should receive training and supervision to ensure that the systems are constantly secure. (When not in use, between shifts, overnight etc) the cost of damage or virus attack on a process system could be catastrophic. Third Party Risk should be kept to a minimum.
Are systems and protective measures in place to prevent any unauthorised access to a process system, if so what are they? Are there response strategies in place?	Elementary safeguards such as password protection, USB port elimination, Firewalls (malware defences) and early warning of abuse are just some of the measures that can be adopted to prevent abuse. Others include the extent to which the network environment of the PCS is separated from the office environment; and the kind of response strategies that have been developed.
Does the Company have a regular System audit programme to mitigate against abuse?	Regular security upgrades, audits and early warning monitoring should be the minimum standard employed. Firewalls are not always effective and to some they represent a challenge to overcome. Links to a national Early Warning System are useful and/or exchanges of information about incidents. The robustness of the defence against undesired and undesirable access by people and malicious software should be tested periodically (penetration tests and red team exercises) (establish ongoing governance).
Does the company have a policy relating to the use of Process Control Systems and if so does it contain a section on Security?	Initial training will instil in users the need to maintain security and to prevent abuse. A cost effective programme should be in place that covers all aspects. Recovery from an attack can at the very least be very costly and could even be terminal. Stakeholder and reputational confidence would disappear overnight.

AREA OF IMPACT:
SYSTEMS

5.8.2 Information Security

Visibility

Low	Medium	High
		X

Performance

This is an area where specific Key Performance Indicators can be set for monitoring breaches of security protocols and procedures, training given to staff and evidence that knowledge is being applied to improve security. These should relate to the risk tolerance of the Company for losses from Information Security breaches and should be reasonable and in line with the peer group. For cyber-security breaches, the level of tolerance will and should be less than for Information Security lapses, but the performance expected of mitigating measures can still be monitored for effectiveness, data loss and recovery.

Definition & Comment

Information Security is a very visible area of interest for most companies. It is often an individual's, computer competence and literacy that dictate the extent of the threat with the majority of incidents attributed to lack of awareness on behalf of the individual. For some companies this area includes the more aggressive cyber-security – the attacks come via computer systems, but the threat is different and can be risk assessed. Advice on cyber-crime is often forthcoming from governments where cyber-security is regarded as a serious and growing problem.

The questions below relate to the measures a Company can install to help mitigate information security, as defined by the Company, and in doing so, have some assurance that the cost of these is appropriate to the level of risk.

Financial Drivers	Impact & Implications
How is Information Security managed in relation to Cyber-Security? Does the Company manage them as a single threat or as arising from different motivations and requiring a different risk management approach?	Given the high profile of both areas of IT related security, there will be a propensity for greater expenditure on each. It is important to apply the Security Risk Assessment process to threat identification and the development of appropriate risk mitigation measures which will vary in extent and cost depending on how serious the threat is regarded by the Company.
How extensive are the measures in place to control IT access?	Depending on the risk identified, a Company needs to invest in managing access, specifying connections that can be made and by whom.
How extensive are the measures needed to meet the Company's internet access policy?	Deciding on how far countermeasures should go in mitigating the threat from social networking will drive the cost. However, limited website access, filtering from different gateways, and ensuring updates are installed are easy and relatively inexpensive measures to take and are particularly if Cloud computing is used.
What is the Company's policy on the removal of data/equipment?	This can be controlled, at a cost, whether issuing encrypted USB sticks, appointing a key user, auditing laptops, ensuring a certain level of encryption, fitting anti-theft devices etc.
How effective are auditing or protective monitoring systems?	If these work, unauthorised access can be reduced. A Company might have a process, i.e. using a log, but if this is not monitored and followed up, it will not work. The analysis needs to take place over time to spot trends and patterns that can then be investigated. Other monitoring such as inspections are also effective but need to be part of a member of the security team, or management's remit. Any monitoring will generate 'false positives' and these will help a process to be fine-tuned.
What are the Company's policies relating to IT and Process Systems access procedures?	Procedures should exist that govern authorised access; passwords; security of systems; security of equipment; security of buildings and housing the equipment. Lax procedures will allow unauthorised access.
What procedures have been adopted by the Company which govern administrators' access?	Administrator access must be limited, strictly controlled and based on a need to know basis. Data removal or Programme alterations may require a double user entry for added security.
Has the Company adopted procedures to be adopted should there be an unauthorised access?	This again is an overlooked area with enormous cost implications; it must be addressed as part of the BCP and have been analysed as part of the BIA. A Recovery Policy should be readily available.
What back up procedures and systems are in place in readiness for use?	Are the Process Systems backed up? What procurement plans are there to replace Process systems and IT?

5.9 Asset Management

Securing Assets is one of most visible areas of financial expenditure. Energy companies have a diverse portfolio of infrastructure Assets under their control, each playing a different role within the overall business process. Whilst some Assets may be critical to the continuing operation of the business, represent substantial investment in technology, people or processes, and be of national or regional economic significance, other Assets might be of peripheral importance or easily replaceable.

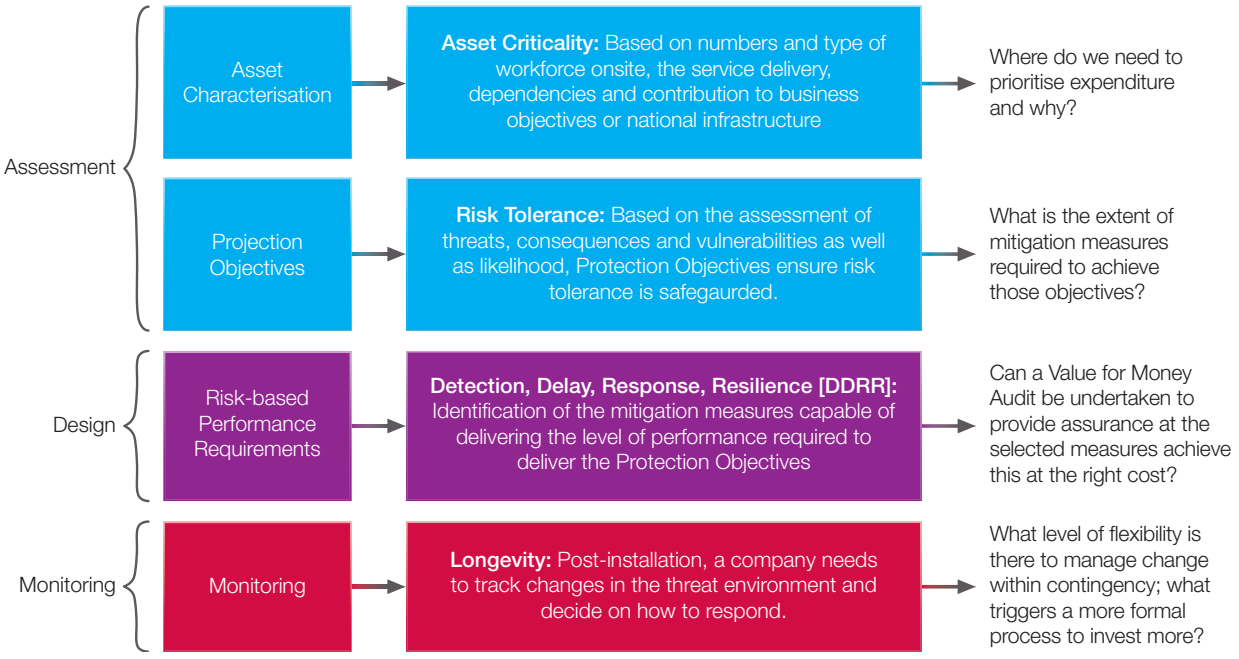
As physical and visible manifestations of a Company's value, security threats often target assets and are the prime focus of attention of the security department when they become aware of potential threats. This is taken account of in a good Security Risk Assesment process as "Threat Attractiveness". For example, protest groups are particularly attracted to assets such as offices and facilities because, from their perspective, it attracts media attention.

There is a direct link between the kind of Security Risk Assessment (SRA) process an energy company uses and the money spent on security. From a security risk perspective, successful Asset Management can be enhanced by an accurate, timely and regularly reviewed SRA that determines the type, nature and severity of risks facing a company's Assets. The SRA process drives the physical, technical and procedural mitigation measures required as part of Asset Management and in doing so there are a number of financial implications that are a consequence of the process – these include the identification of single points of failure and application of focused, flexible and cost effective security measures at Company Assets that will also support operational activity.

Depending on the type of Security Master Planning methodology used, there are a number of 'filters' (primarily found in the areas of Assessment, Design and Monitoring) that may allow the potential spend to be better analysed, approved with greater assurance and subsequently monitored with confidence. These are shown in Fig. 5.9.1 below.

Furthermore, Asset Management can be enhanced and made more cost effective by the use of a Value For Money (VFM) process that judges whether resources are being used to optimal effect and to achieving the desired outcomes. The VFM process is covered in Box 5.9.1 and Fig. 5.9.2 below.

Fig. 5.9.1 Financial 'Filters' Embedded in a SRA process [1]



AREA OF IMPACT:
ASSET MANAGEMENT

5.9.1 Offices

Visibility

Low	Medium	High
		X

Performance

The security measures introduced to protect Assets should perform to a specified standard in order to provide assurance that risk has actually been reduced as expected from the expenditure at the outset. Phase C of PRISM® sets out how performance-led design standards can be applied around the four elements of Detection, Delay, Response, Resilience ("DDRR") and each Company should define what these are as a consequence of the Security Risk Assessment process set out in Phase B of PRISM® which sets out the requirement of those measures and their appropriateness.

Definition & Comment

Security of offices includes everything from securing the people working in the offices, the office property itself, the proprietary information and the reputation of the company. Examples of these measures are the installation of an 'Integrated Security System' or ISS, security of staff, security of information technology equipment, HR records, vital historic documents and legal documents. It may also include other proprietary information such as security of patents, customer and client lists. Loss of any or more of these records will impose a financial penalty on the company. Security of personnel is paramount together with the reputational penalty due to loss. Companies also suffer media loss due to excessive intrusion.

Financial Drivers	Impact & Implications
Does the Company have a fully functional 'Integrated Security System' in place?	This includes features such as Perimeter Fence and PIDS, Access Control, Alarm Assessment System (CCTV), Security Lighting, Intruder Detection System, all encompassing building hardening and system management. There are serious financial implications to enhance existing security. How is the building divided by security zones (public, semi-public, controlled and restricted zones)? Modernisations should be designed and audited to ensure they are Fit For Purpose and reflect Value For Money.
Are the existing systems audited to identify weaknesses? Are faults listed and rectified?	If weaknesses have been identified, are they also remedied? Are there maintenance and service contracts in place? Are there auditable records of system activation or malfunction in place?
Has a Critical Point Analysis ("CPA") been carried out in order to identify those parts of the Offices that are critical to the functioning of the Company?	Following on from the CPA, has a Business Impact Analysis been undertaken and incorporated within a Crisis Management Plan? Are there any Fall Back alternatives?
What Security Policies exist to enhance and ensure the protection of the staff?	Does the Company organise Security Awareness Workshops for the staff? How are the security inductions organised? Other important areas are: Vehicle Access Policy; Traffic Management System; Vetting Policy; Mail Room and Post Policy; Bomb Warning Policy; Search Policy; Evacuation Policy; Visitor Policy; Goods in/out Policy; Waste Disposal Policy; etc. What arrangements exist for Staff and Visitor Car parking? Is there an off-site receiving dock where all deliveries can be properly checked? Policies and procedures are needed for all of them.
Has the Company undertaken a review of the possible Single Points of Failure and taken steps to mitigate the risks?	All these groups or clusters can be seen as Single Points of Failures (SPOF): Water, Gas, Electricity and Sewerage, IT, Telephones and Communications, Transport and Logistics, Customers and Clients. Staff sickness during pandemics together with any unforeseeable natural disaster.
What policies exist to ensure the protection of proprietary information?	Is proprietary information restricted to certain areas or is there wide access to such information? What is the policy regarding visual access to proprietary information while contractors, vendors and visitors visit the Company? What are the policies regarding marking and storage of proprietary information?

[1] *For example as set out in Phase B of PRISM®*

AREA OF IMPACT:
ASSET MANAGEMENT

5.9.2 Sites/Facilities

Visibility

Low	Medium	High
		X

Performance

As with 5.9.1 the same approach is required to define specific Performance standards for equipment both in relation to cost and effectiveness. In addition in some sub-sectors, the Value for Money audit process can allow a Company to recoup some, if not all, of the cost associated with specific security measures deemed necessary, often for Assets deemed part of the CNI of the country the Asset is in.

Definition & Comment

Security of sites/facilities incorporates a lot of the security measures installed to protect the offices. Other cost areas within sites/facilities might include process areas, storage, metering, dangerous substances, loading and unloading points, all of which should be reviewed. Surrounding areas should also be taken into account as they can be used to gain access to the main site/facilities.

Financial Drivers	Impact & Implications
Does the Company have a visitor site access policy?	Site visitors will be a drain on resources, constantly be a security and safety risk and require continuous management throughout the visit. Visitors should be discouraged unless absolutely necessary. Security Vetting of contractors, vendors and visitors must remain a consideration along with site escorts, badging and signing in and out. Are visitors logged? How long are these records kept for? Is there a policy to alert site managers of impending visitors? What screening is necessary for employees, contractors, vendors and visitors? What policy is in place regarding on-site vehicle access?
Has a CPA been undertaken and assessed in line with Security Risk Assessments?	The level of Criticality alongside the Threat Level and Risk Appetite will determine the degree of security enhancement necessary on any one site. This must not be generic but must be site specific. Before any costly enhancement programme is begun Value for Money Auditing should be adopted to ensure that value and efficiency is obtained. Is there a Disaster Recovery Program in place?
Have the sites been subjected to an attack scenario assessment and Gap analysis?	Regular assessment and analysis will show up deficiencies and highlight areas in need of modernisation. Although this will remain an ongoing expense it will ensure that the system remains totally functional and capable of securing the site.
Does the Company have an Automatic Access Control System (AACS) in place?	This allows authorised access to those in the correct roles, but must be updated and reviewed regularly. Is there a key management in place? What is the AACS used for and who operates it? How long are the records kept for?
What is the process for ensuring security passes are generated and worn?	This varies a lot – the quality, style and entry systems dictate the cost but critical areas should remain secure 24/7 with access only by the use of the AACS.
What sign off is required for issuing a pass?	Sometimes this can be joint between HR and Security. A document verification check can also be required.
Does the Access Control System produce a Muster List of Personnel on site, for use in case of an Evacuation?	Modern AACS are capable of multi tasks such as Muster Lists; Authorised Access Control; Loss Alert; Tamper Alert; Misuse Alert; Security of rooms, areas, buildings, premises or sites will be increased by the use of Access Cards or Tokens with PIN's. Access to departments, offices, floors, production and process areas can be changed quickly and efficiently. Misuse can be identified with additional training given. Are the security officers trained to request these details in case of an emergency? Is there a law enforcement liaison in place in case of an emergency?
Are there any measures taken to secure the surrounding areas of the Company?	Companies in the same area often work together and set up an alert system. Is there a system to contact neighbouring companies in case of an emergency? Are there any other measures taken to secure the surrounding areas such as extra cameras, patrols, etc? What about natural perimeter defences such as storm walls, water barriers and so forth? Is the landscape near the building lighted in order to display the actions of anyone near the buildings?

Box 5.9.1. Value for Money Auditing in the Energy Sector

Value for Money (VFM) auditing embraces the principles of economy, efficiency and effectiveness. A VFM study focuses on a specific area of expenditure and its primary aim is to reach a judgment on whether Value For Money has been achieved or not. Value For Money is defined as the optimal use of resources to achieve the intended outcomes of a specific project.

Within the energy sector, companies are facing emerging government requirements to strengthen protective security around their sites and assets to secure the energy supply. In some countries the cost of these security enhancements required by the government is refunded to the energy company through pricing mechanisms approved by the energy regulator. To avoid excessive public money spending and wide cost variances, Value For Money audits are designed to provide assurance that the security measures installed at a site fulfil the demands of the operator as well as other stakeholders. They ensure a consistent approach to all sites and assets that form part of the supply chain. The VFM process benefits both the operator and its stakeholders as it provides assurance that funding is being used as intended with no unnecessary waste and the allocated funds are used responsibly.

By implementing the VFM process, owners and operators of energy infrastructure assets will have assurance that the security measures are at market value and in line with the requirements set out.

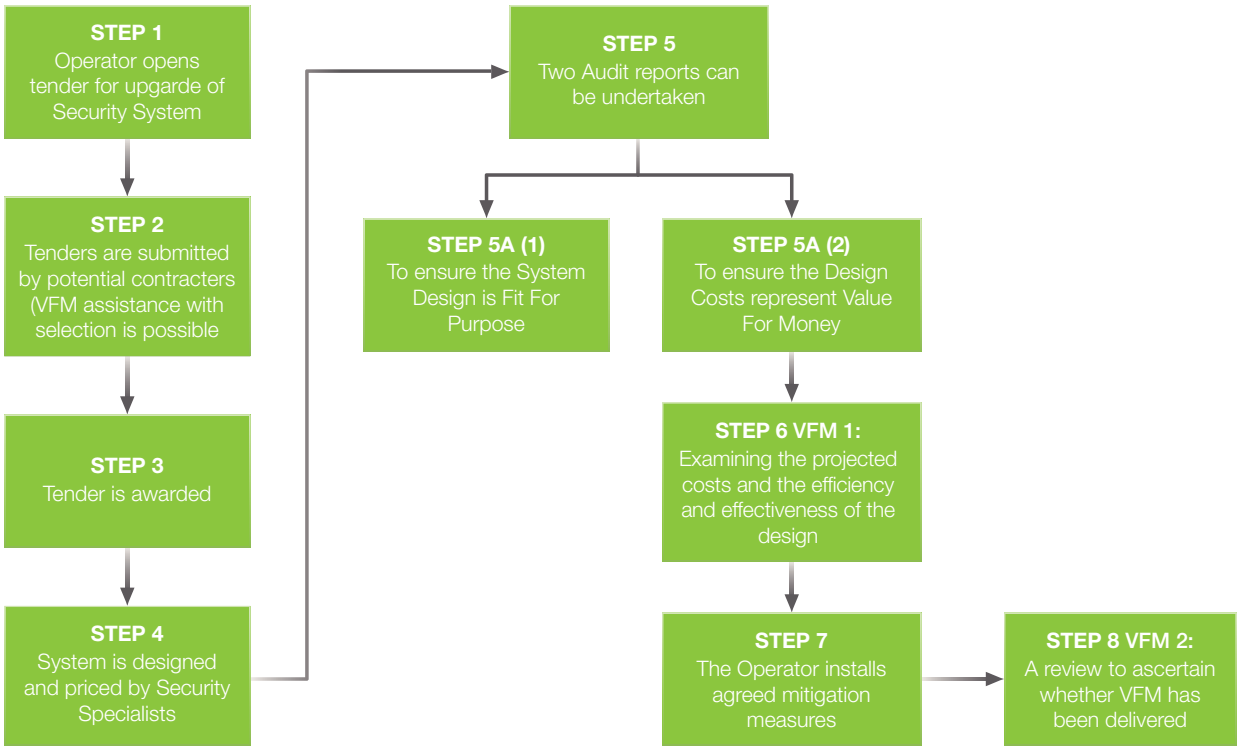
Assurances should be given to stakeholders that the system is being designed and installed economically; in an efficient manner and providing a level of effectiveness which will generate an enhanced level of confidence in the result for an extended period of time. By ensuring value for money, stakeholders may show increased willingness to support projects confident in the knowledge that every effort is being made to control spending in an environment that, historically, has not been as careful as one would expect.

Benefits of the VFM process:

- Ensuring a consistent approach across the supply chain
- Establishing an efficient security process
- Producing cost effective results
- Creating an end result that is both Fit For Purpose and Value For Money
- Providing stakeholders with assurances that the system is being designed and installed economically
- Generating an enhanced level of confidence in the result for an extended period of time.

Fig. 5.9.2 shows what the process looks like in practice.

Fig. 5.9.2 A Value For Money Auditing Process



5.10 Planning

This Section explains the importance of planning **from a security risk perspective**, the areas that need to be covered as part of security planning and the associated financial implications of these activities. Given that Corporate Strategy is the single most important influence on the security exposure a Company faces, the Security Strategy and associated planning processes must be up to the task of supporting and protecting the delivery of that Corporate Strategy as well as being capable of evolving to capture and respond to change.

The Security Planning process can encompass a wide scope of planning activities that cover the spectrum from risk identification – monitoring – response – recovery – resumption. (See Fig. 5.10.1) Given the profile of security risk management in many energy companies it is not uncommon to find the process dominated by Business Continuity Planning and Crisis Management. So a Company needs to takes a 'helicopter' look at all the plans generated across its business and make sure they are joined-up or aligned to deliver a seamless management process covering that planning spectrum and reflect any duty of care or legal requirements. As this rarely happens, **Security Planning in energy companies can be fragmented and may not benefit from the expertise that can exist in other more visible planning areas**.

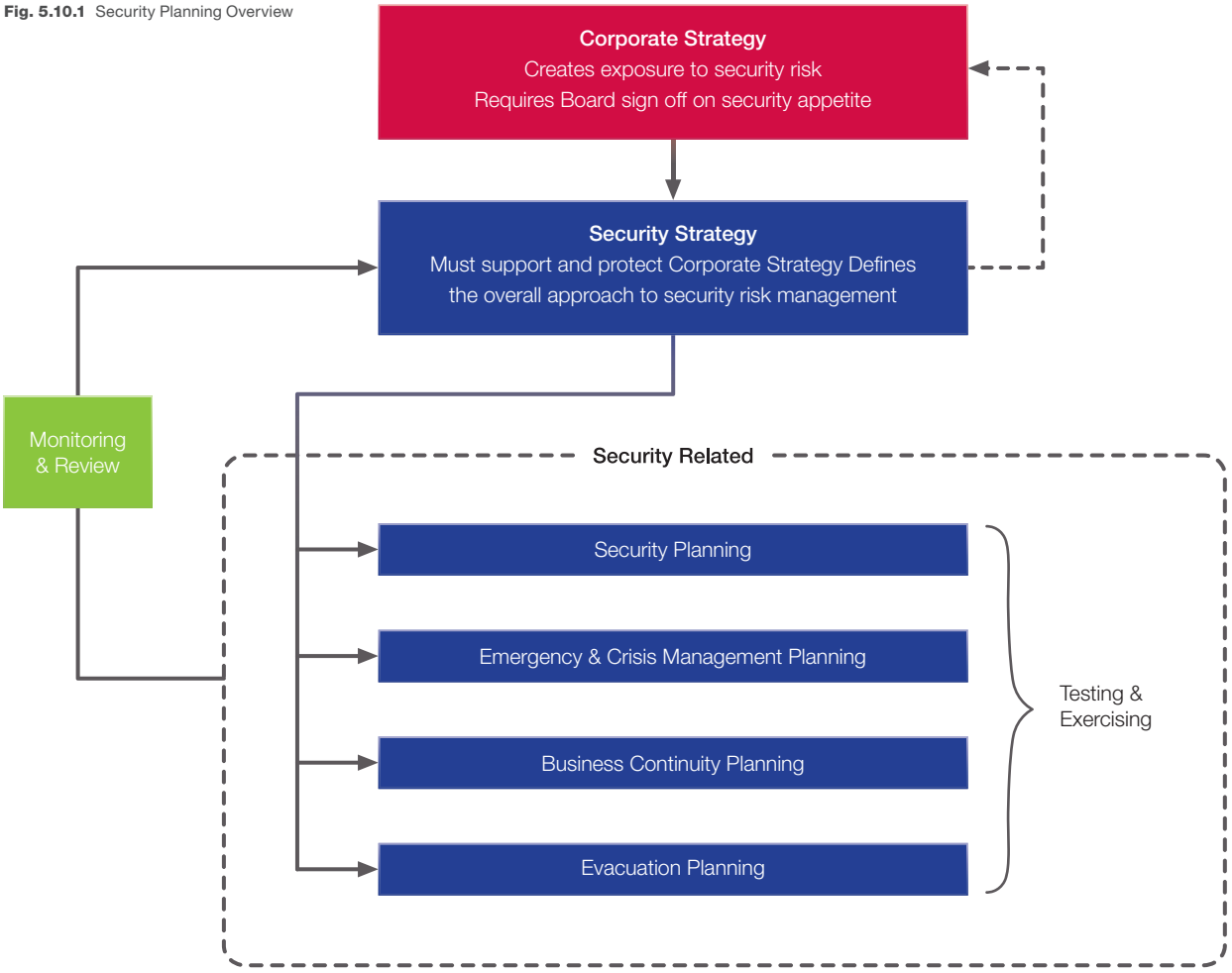
It is only when security risks are realised that the true worth and indeed the effectiveness of Security Planning and related Plans becomes apparent. Plans may face a number of tests which may manifest themselves individually, as an escalating scenario or, in a 'worst case' situation, a rapid confluence of events, but how well they manage the situation and deliver what is expected is the key performance measure for all plans.

From a financial perspective, effective security planning will reduce the direct and indirect consequences of security events on assets, personnel and reputation. The opposite is true. Poor security planning can lead to ineffective mitigation measures that do not protect assets and personnel and require expensive remedial works to put right. A slow and disorganised response to, management of and recovery from, security events can also cost the organisation unnecessary loss of revenue, physical assets and access to markets as well as damage to reputation.

Security planning in itself incurs cost. Aside from the need for personnel (either from within the company or using outside consultants) to develop Security Plans, there are costs involved in testing the Plan(s) and reviewing the outcomes. It may be necessary to invest in equipment, personnel and infrastructure **that will facilitate** the emergency and crisis management process as well as the need to enter into standing contractual agreements with outside parties in order to support activities such as evacuation operations.

Security planning can be viewed as an insurance policy – ensuring that if security risks become manifest, the Company has the capability to mitigate their immediate effects, manage the consequences and facilitate an organised and timely return to normal operating conditions.

Fig. 5.10.1 Security Planning Overview



AREA OF IMPACT:
PLANNING

5.10.1 Strategy

Visibility

Low	Medium	High
	X	

Performance

The performance measure here is whether or not the Corporate Strategy includes choices that reflect consideration of the security environment and risks to the business. The planning process should capture an assessment of security issues within the business and allow for a consolidated review of risk generally across the Group. In many companies, once all the business segment plans have been aggregated, the aggregate risk that results from those plans can then be identified for the Group as a whole. The same needs to be evident for security.

Definition & Comment

The Security Strategy is derived from the Corporate Strategy as it is this that creates the security exposure in the first place – where and how a Company decides to create shareholder value. The Corporate Strategy is a consolidated view across any number of profit centres (depending on structure) and the Board of Directors needs to know and sign off on the consolidated amount of risk they are exposing the business too, in order to deliver that strategy. This is not just security risk, but also HSE, Legal, Reputational and Financial.

Financial Drivers	Impact & Implications
At what point in the planning process are security risks considered and decided upon?	Are there guidelines issued that explain to the profit centres how to identify and evaluate the security risk exposure of their current and planned activities over the strategic planning period? Or is there an assumption by the business areas and corporate support areas that this is covered by the Security Director or Manager? Is there any engagement with those engaged in preparing the Corporate Strategy plan updates every year? Do they know how the overall risk exposure to security threats is consolidated and viewed? For example, if the company faces threats from say Greenpeace – do they look at the threat across the business as a whole, or just around the locality where they have reason to believe that threat exists?
Is the process 'fragmented'?	If looking at security threats across the Company as a whole is done outside of the strategic and business planning process, then it is done in parallel. At what point do the lines cross? This is crucial because the Security Strategy cannot exist in isolation, it must reflect and be implemented by, those responsible for it. It is a costly and unnecessary process to align the processes that focus on reward, and the risks associated with achieving it.

AREA OF IMPACT:
PLANNING

5.10.2 Emergency & Crisis Management

Visibility

Low	Medium	High
		X

Performance

The emergency and crisis management plans should meet Corporate standards and testing them should be a regular performance measure and would identify any gaps. Those responsible need to have a well developed process to generate the plans and ensure they meet best practice standards and have the support and visibility with the business they need to be deployed effectively.

Definition & Comment

Emergency & crisis management requires measures in place to prepare for, mitigate, respond to and recover from unexpected events that disrupt activity. The focus is not on what might cause an event to occur and the probability or likelihood of occurrence, but the actions that need to happen to deal with an event swiftly and effectively.

Putting any of the plans noted in this section is a time-consuming exercise and can involve many internal and external stakeholders. So the process needs to be efficient and joined-up. Good emergency and crisis management requires an infrastructure of control rooms, telecommunications, reliance on key suppliers, good communications and reputational management – all of which would be tested in an emergency and crisis situation which can be referred to as a 'perfect storm' that tells a Company how good it is at responding to and mitigating a security risk that materialised.

Financial Drivers	Impact & Implications
Is there a single point in the Company responsible for the co-ordination, planning and management of emergency and crisis management? Are there specific, identifiable costs associated with putting in place the support required to implement the plan as anticipated?	Companies approach this differently – there is no one good model, it depends on the Company's structure, the types of assets it has, their location and the resources available to it. There may be local requirements, access to assistance, quality of emergency services etc in different countries that dictate how this should be managed, and the costs involved in doing it well.
Has training been undertaken, in particular in media management, from the most senior member of the management team to spokesmen on the ground?	The communication requirement for implementing a Security Strategy runs through each area of impact, but it is particularly relevant here where the quality of the planning and time invested in delivering it, coincides with reputational management. Good media training costs money and needs to be undertaken and re-done regularly.
Does the Company emergency & crisis management plan take account of the core constituent parts of preparation, mitigation, response and recovery?	In order to be operationally effective, the Company's emergency & crisis management plan must include the actions required before, during and after an emergency or crisis and the associated inputs and outputs that will drive the emergency & crisis management response cycle. Preparedness for emergencies and crises and implementing related plans will cost money. The management of emergencies and crises is cyclical and thus may have to be repeated over a prolonged period until the conclusion of the event and a return to normal operations.
Has the Company established an emergency & crisis management checklist?	The requirements of an effective emergency & crisis management plan are varied. The establishment of a checklist, to be used and reviewed regularly, will improve efficiency through highlighting areas of weakness, gaps in capability and establishing responsibilities.
Are other business areas aware of their emergency & crises management roles and responsibilities?	An effective emergency & crisis management plan requires input from a number of business areas such as IT, personnel, HSE and logistics departments. From a practical perspective, this input will require departments to supply personnel to the crisis management team as well as providing physical assets where necessary. There are departmental cost implications in these activities.

AREA OF IMPACT:
PLANNING

5.10.3 Evacuation

Visibility

Low	Medium	High
		X

Performance

Testing and exercising is another key performance measure which should identify any gaps in the planning process. Group standards in Evacuation planning that reflect best practice in the peer group and from past experience in the Company will aid the effectiveness of individual plans, but ultimately, testing the Plan is crucial to knowing if planning assumptions and the preparations made, will hold in an evacuation situation.

Definition & Comment

This is noted separately but is, of course, fundamentally linked with the above. The Company should have in place the capability to conduct an orderly and coordinated evacuation of assets, operating areas and countries if it is deemed that the security situation warrants such action. Evacuation has several financial drivers. For example, making sure transportation routes are available with third party input, the cost of re-locating staff and office equipment in another location for an unspecified length of time. The cost implications should also be looked at as part of the BCP process because they influence how quickly the operational activity could be resumed and the opportunity cost of suspension during the period leading up, during and after an evacuation has been deemed necessary.

In some environments, Companies can collaborate and coordinate evacuation procedures which will be done to strengthen the implementation of the Evacuation Plan rather than necessarily to save cost, although this may be one outcome. Whilst desirable, it is important to make sure that any duty of care or legal risk issues are identified beforehand and agreed by the Legal Department so that, if such collaboration does occur, not only are the practical and financial benefits known in advance, but the potential risks and uncertainties are too.

Financial Drivers	Impact & Implications
What authority is given locally to source, assess and pay for what is needed to deliver the evacuation plan?	Does the Company know how much it spends on ensuring its evacuation plans are capable of implementation? How is that captured, as part of the budget, as a contingency or a separately funded item?
What contingencies are in place? How well have they been verified and risk assessed?	This is in part related to the above point but evacuation planning, as with emergency & crisis management planning, requires expenditure on equipment and assets that might never be used such as communications equipment and associated ancillaries, medical supplies, rations, stockpiling of supplies (which may require warehouse storage and periodic replacement and/or rotation of said supplies), maintaining cash floats and spare fuel. For transportation related points see subsequent points. Also there are occasions when an evacuation cannot be conducted – for example, is there sufficient life support in situ if a 'stand-fast' has to be ordered? Do Company Assets require expenditure and modification to support a 'stand-fast' such as safe rooms and provision of guarding?
To what extent can existing Company Assets be used as part of the evacuation plan?	Does the Company know if existing road, maritime and air assets used during normal operations would be sufficient (and available) to conduct an evacuation? Further investment may be necessary either to establish that Company Assets alone can conduct evacuation or to create a sensible balance between 'in-house' Assets and alternative providers (see next point).
What extent is the back-up?	Making sure there are several alternatives in place will cost more, but usually with evacuation planning, the risks of not being able to respond effectively are so great many companies will invest the time and money to get it right.
If co-operation with other parties is deemed necessary, have the legal implications been considered in the Plan?	There can be an inherent legal risk IF any type of sharing arrangement is not understood before it comes into play. To what extent are evacuation plans shared with other operators, not simply to gain any potential economies of scale from limited resources (ie chartering a larger plane to be on stand-by) but also to make sure the right legal checks have been identified and planned for.

AREA OF IMPACT:
PLANNING

5.10.4 Security

Visibility

Low	Medium	High
		X

Performance

The key performance measure is whether or not the Security Plan will enable the business to implement the Security Strategy and the objectives contained therein. If there are financial constraints on security expenditure around certain Assets or for Company-wide procedures, for example on screening, then the Security Plans need to be within budget and make a good case for that expenditure. Where the business or HSE funds security spend, the challenge is to a) identify what that is across the Company as a whole and b) identify the other areas where expenditure can occur. This is, of course, the purpose of these Guidelines.

Definition & Comment

The Security Plan sets out how the Security Strategy is to be implemented in support of the Corporate Strategy. The Security Plan will recommend a range of enhancements or improvements to security measures in place around specific Assets and will include physical, technical and procedural measures. These should be the outcome of a good risk assessment process that identifies the scope, nature and severity of security risks facing the Company with approved protection objectives. In some countries and with designated CNI assets, the Company may have little choice over the extent of measures required, in other instances, there is greater discretion.

As noted earlier, the RSMP is a guide about how to put together a good Security Management Plan.

Financial Drivers	Impact & Implications
What security risk management methodology is the Security Plan based on? Are there Corporate-wide templates and guidance notes for each Asset or locality to aid completion of the Security Plan.	The use of a consistent and robust framework for security planning will provide confidence that security risk is being managed in-line with best practice and that financial decisions made as a result of this planning (for example expenditure on mitigation measures) are both necessary and represent value for money. Furthermore, such an approach provides an auditable process for internal and external stakeholders.
Where is the most investment in security measures?	What elements are allocated to OPEX and CAPEX and what is spent on these each year? How are the allocations categorised – i.e. training, maintenance, post delivery service agreements, induction?
Who is responsible for the budget?	Often the Security Director or Manager is not the budget holder so there are competing pressures on funds – so the stance of the Company on security is critical in terms of what gets approved (with procurement's support) and what does not.
CNI enhancements as prescribed by government.	Where the Company has to implement security enhancements as part of a government CNI program, how is this funded and is there a cost recovery process?

AREA OF IMPACT:
PLANNING

5.10.5 Business Continuity Planning

Visibility

Low	Medium	High
	X	

Performance

There are standards adopted in most companies for BCP and the scope should be evident along with references to other related plans that cover security issues. A key performance measure will be whether or not the BCP for each Asset is linked into other plans that relate to security so that there is assurance that security risk events and incidents are going to be managed to the standards applied to BCP in the Company.

Definition & Comment

Business Continuity Planning (BCP) represents a managed effort to identify significant threats to normal operations, prioritise key business processes and plan mitigation strategies to ensure effective organisational response to the challenges that occur during and after a crisis.

There are close links between all these plans, and the scope of each needs to be delineated clearly (bearing in mind they should all be linked to the single security risk monitoring model). BCP really kicks in post-event to get the business up and running quickly but it can also identify the causes of business interruption and focuses on key and critical systems. So it does include an impact assessment, but it does not go into the detail on the root cause, nor would it look at the competitive impact of down-time.

Financial Drivers	Impact & Implications
Has a Business Impact Analysis been carried out?	This analysis will set the format of the BCP by taking the Risk Register and providing evidence of how the business will react to a number of given scenarios. The scope of the business impact analysis can be link to security planning to aid decisions about appropriate mitigation measures.
What is the scope of the BCP in the company and to what extent is it linked into other plans also dealing with the impact of a security event? How consistent is the BCP process across the Company, are there Group standards or does each region have its own approach?	Any duplication costs money. Having an integrated link between all these plans is important with the triggers clearly identified and monitored via a single model. How close is the link between IT security and BCP?
What level of support exists for ongoing BCP?	As with other elements of security planning, BCP is an ongoing process that needs to be supported by senior management and funded appropriately.

AREA OF IMPACT:
PLANNING

5.10.6 Testing & Exercising

Visibility

Low	Medium	High
		X

Performance

Once plans have been agreed – the key measure of performance is how well they work when tested – either live or in a pre-planned exercise. Again, expectations should have been set at the outset which reflect duty of care and legal requirements, stakeholder expectations, Group risk tolerance and strategic objectives. These create a framework that the plans must deliver within.

Definition & Comment

Testing and exercising Security Plans ensures personnel are aware of their roles and responsibilities, it can reveal weaknesses in procedures and communications, give confidence in the accuracy and completeness of plans and lend credibility and authority to those in crisis management positions. The scope, frequency and depth drive the costs of testing and exercising. Given that all the Plans referred to above need to be tested regularly, the following questions relate to all of them and the potential costs involved.

Financial Drivers	Impact & Implications
Who decides what should be tested and when?	How is the scope defined?
Is there separate budget agreed for this?	How much is it and how is it spent?
What type of testing and exercising is conducted?	There is a big difference between the costs of 'table top' and 'live' exercises the latter of which requires extensive planning and organisation and can include interdisciplinary and multi-agency input. Large scale exercises may temporarily reduce operational output and tie up personnel. How often are exercises conducted and how long do they last?

Chapter 6
Corporate Competencies for Managing Security Risk

6 Corporate Competencies for Managing Security Risk

Having set out the Guidelines for each area involved in implementing the Company Security Strategy, it is worth remembering that the skills and competencies required to propose, plan and manage the right response to that risk are generic and evident in any corporate environment.

These are shown in Table 6.1. These core corporate skills and competencies will assist individual departments and business units to identify, evaluate and manage the impact of security risk on their area and the financial implications.

Companies have an opportunity to develop a 'corporate competency' in security risk management that reflects ALL the experience across the business required to deliver a joined-up risk framework.

This would not only include a security risk governance framework, a performance-led risk assessment process and an integrated monitoring and reporting model, but also the competencies set out in Table 6.1. Together, this will provide the Board with an assurance that security risk is understood by all and being addressed proactively across the organisation.

It should be noted that whilst there are generic skills and competencies that all business units can apply to the management of security risk, **business units should not attempt to operate in isolation**. Close liaison with corporate security is essential in order to establish that business units are following a consistent and agreed approach based on best practice and that specialist subject matter experts, needed for activities such as Security Risk Assessment, Security Design and Implementation and Review, are utilised. This can all be encompassed within a Core Competency framework for security risk.

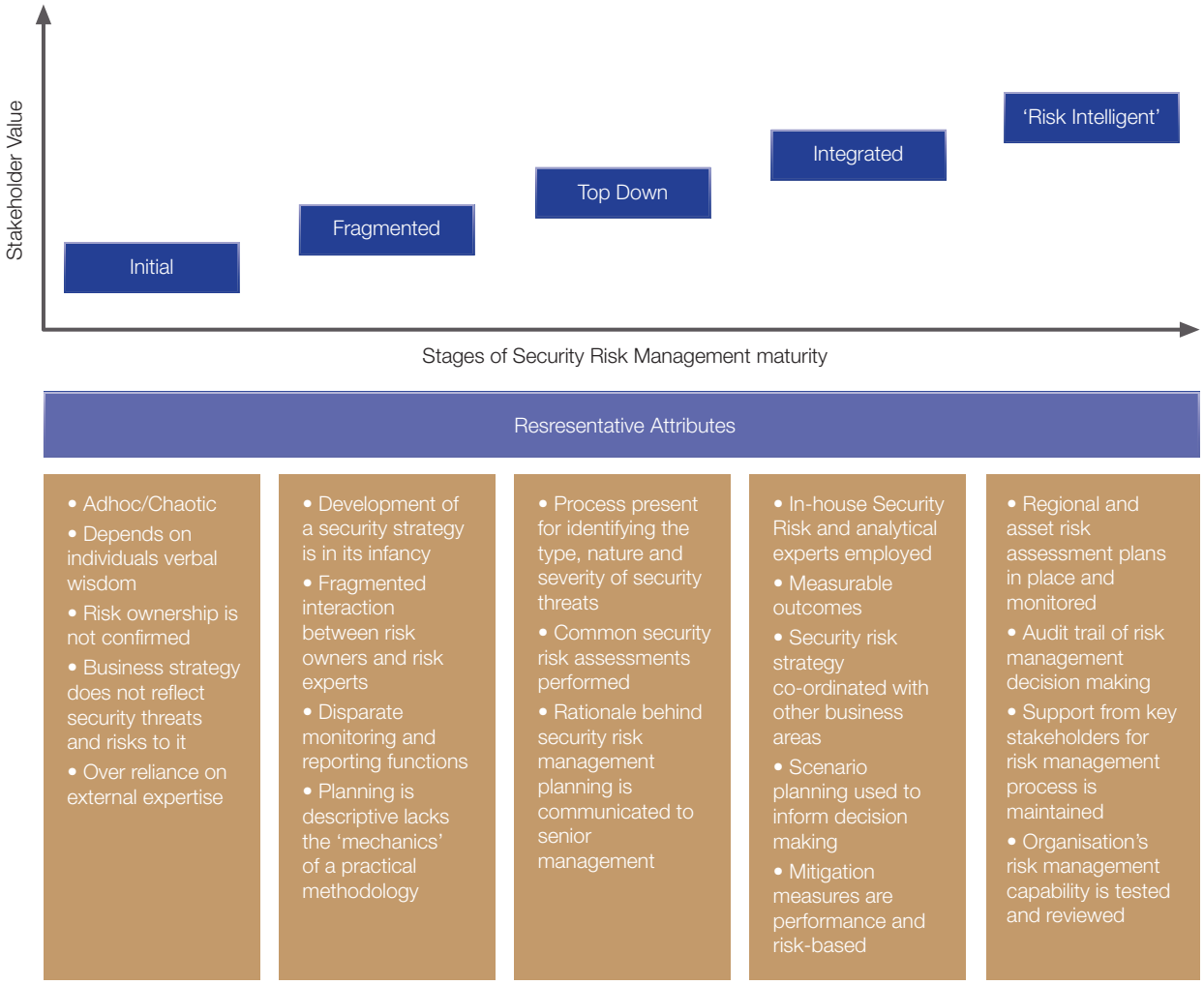
Table 6.1
Corporate Competencies for Managing Security Risk

Generic Skills/ Competencies	Resulting Outcomes, Requirements & Knowledge
Risk Analysis	• Identifying security risk consequences of business unit actions. • Scenario planning/horizon scanning. • Potential risks identified and risk/reward balanced. • Agreed risk indicators/triggers to link into monitoring framework? • Compliance with organisation codes of practice/directives, regulatory and legal requirements. • Development of professional networks. • Sharing common thinking with peers – understanding what they are doing about security risk.
Monitoring & Review	• Framework in place for monitoring security risk at business unit level. • Regular meetings to review security risk consequences of business unit activities. • Planning assumptions reviewed. • Awareness of PESTEL developments in business unit sector and areas of operation.
Communication	• Accuracy, brevity, clarity. • Development of consistent messages. • Information sharing practices. • Regular liaison with security manager/department/risk manager. • Regular liaison and coordination with other business units. • Development of professional networks. • Securing senior management support for security risk initiatives.
Process & Procedural Development	• Are there risk management policies and procedures in the organisation and is the business unit familiar with them? • Is the business unit decision making process auditable? (on the basis that every action can have a process wrapped around it to make it so).
Planning	• Written up and approved Plans under an integrated security risk management framework. • Specific and agreed resource allocation. • Are business unit activities within the organisation's risk appetite or referenced to a defined risk appetite and business need. Future business unit activities – are security risks part of planning activities (see 'Identification & Evaluation). • Scenario planning.
Stakeholder Analysis & Engagement	• Stakeholder Engagement Plan. • Management of expectations. • Appropriate, consistent and timely communication. • Review to capture change in people, organisations and interests. • Identification of internal and external audiences.
Leadership & People Management	• Responsibilities and roles identified and allocated. • Development of risk management techniques. • Pursuit of improvement. • Key messages on security risk strategy and positioning as a priority. • Demonstration of the security risk culture. • Maintain individual and business unit security risk competencies.
Development of Security Culture	• Security risk education and training programmes. • Relevant training courses for staff. • Maintain familiarity with security risk best practice. • Demonstrable examples of what a good security culture looks like; and what it is not.

The Author acknowledges that every energy company will already be exercising some elements of a coherent security risk management strategy, but as expected in a sector as dynamic as energy, continual improvement is a key attribute of corporate success.

Fig. 6.1 outlines the stages of 'Security Risk Management maturity' and the corresponding representative attributes that may be found within an organisation. Deciding the right approach for an energy company needs to be taken where accountability lies, at the top of an organisation.

Fig. 6.1 Stages of Risk Management Maturity



Chapter 7
Summary

7 Summary

The RSMP and the PRISM® process it is based on, will define the Security Strategy that will deliver the shareholder value an energy company wants to create. The Guidelines will tell the finance director what that Security Strategy is going to cost the business.

Many energy companies do not know what their global security exposure is, let alone what the cost of managing it is. Given the risk environment and governance pressures on companies in the sector, that cannot be sustainable.

It is possible to identify the true cost of securing assets and infrastructures in the energy sector. It is also possible to expect results and measurable outcomes from that cost that reflect a board of directors' attitude to risk and reward. Using PRISM® and the Guidelines, an energy company can do both.

The Guidelines are not trying to explain how to undertake security risk assessments or how to undertake BCP and other planning activities. **They are an aid which can be used by a Company to identify the true cost of implementing the Security Strategy that will allow the Corporate Strategy to be delivered**.

The questions are not meant to be exhaustive, but to provide a signpost for further enquiry and challenge to ensure a Board of Directors know what it will cost to manage its aggregate security risk. **This is a key requirement and the risks of not knowing more than outweigh the cost of finding out!**

Harnser Risk Group
Autumn 2012

The Author would encourage an energy company **to create its own set of Guidelines** from those provided here, so that it has a bespoke process in place to develop its own Security Strategy.

This will give the Finance Director and the Board of Directors a clear understanding of the true cost of managing the security threats to its Assets, now and in the future.

About the Authors

Harnser Risk Group is an international specialist in **security risk management** working for multi-national organisations, governments and commercial companies in the Energy and Transport Sectors. It operates in **Europe** and the **Middle East** through its Headquarters in the UK and Oman.

Its advisory work is based on the award-winning **Performance and Risk-based Integrated Security Methodology (PRISM®)** and falls into several categories:

- To advise on **CNI Security Strategies** with national governments.
- To challenge traditional thinking about security risk by engaging with a wide range of **stakeholders**.
- To support security specialists working in Companies to position security risk as a **business enabler**.
- To **design complex technology-based solutions** that meet **performance and risk-based standards**.
- To **ensure value for money** investment in security infrastructure for governments and companies.
- To implement security **risk assessments** either as part of PRISM®, or as part of **Due Diligence.**
- To advise clients as they seek to **secure visibility, funding and support** for security risk investment.

www.harnsergroup.com
www.prismworld.org

Harnser (UK) Ltd
69-75 Thorpe Road
Norwich NR1 1UA
United Kingdom

T +44 (0)1603 230534
W www.harnsergroup.com
W www.prismworld.org

Designed by **Mearns & Gill**