

CORPORATE DEFENCE: RISK MANAGEMENT, BUSINESS RESILIENCE AND BEYOND

Abstract: Corporate defence represents an organisation's program for self defence or self-protection. This paper explains the concept in more detail and explores where business continuity fits into the corporate defence paradigm. The changing nature of corporate defence in the 21st century is discussed and the resulting opportunities which present themselves for those involved in business continuity initiatives are identified. The paper is designed to provoke a certain degree of thinking outside the box and to encourage future progress in this area.



Author: Sean Lyons, Principal, R.I.S.C. International (Ireland). Sean is currently regarded as a leading pioneer within the contemporary corporate defence movement. He is the resident contributor in the field of corporate defence for the RiskCenter, a New York financial risk management media company, based on Wall Street. Sean has two decades of experience in the banking and financial services industry, working as an operational troubleshooter, internal auditor and management consultant.

Introduction

What exactly does ‘corporate defence’ have to do with business continuity? During this paper we will be looking at the changing nature of corporate defence in the 21st century, and the resulting opportunities which present themselves for those involved in business continuity initiatives. This paper presents a high level view of the developments occurring in this field and is designed to provoke a certain degree of thinking outside the box on this topic, and to encourage future progress in this area.

What does corporate defence mean in your organisation?

Although the term corporate defence may be somewhat intuitively understood, its precise meaning can vary from individual to individual, and as a result its priority within an organisation can also vary, hence the saying “doctors differ and patients die”. For now let’s just say that corporate defence represents an organisation’s program for self defence or self-protection. Initially I would like to present two contrasting views of corporate defence, and readers can best decide for themselves which of these views most closely resembles their own organisation.

The traditional view

Firstly we are going to address what is often referred to as the traditional view. From my own experience in conversations with senior executives regarding the topic of corporate defence, this conversation is generally restricted to either that of security or litigation. This unfortunately represents a very narrow view and a somewhat restricted focus, as corporate defence has in fact a far more comprehensive brief. The traditional mindset is generally one of a reactionary nature, where corporate defence issues only appear on the radar, after a serious incident has occurred, which has more than likely already attracted executive attention. Indeed, in this environment priorities tend to fluctuate on a daily basis, in a direct response to the most recent incidents, and for some this can be a very frustrating working environment. In an organisation with a traditional view of corporate defence, defence related activities tend to operate in silo type structures. This means that they are not in alignment with one another, but rather they operate in isolation. There tends to be little or no interaction, sharing of information, or indeed collaboration. Frequently there is also very little cross-functional support among these activities, but rather they can very often be the subject of internal power struggles. As a consequence of this type of traditional mindset, an organisation can be subject to typically negative results. Generally this type of attitude can result in an organisation operating in a crisis management mode, whereby it finds itself continuously fire fighting on a daily basis. Very often the overall responsibility and accountability for corporate defence is dispersed or fragmented, diluted or ambiguous. In certain scenarios it can sometimes even be non-existent. This can obviously result in omissions or gaps, and these in turn create vulnerabilities which can later be exploited, rendering many other related efforts ineffective in the process. All of the intersection, duplication and overlap of activities which can occur in the silo type environment can also result in considerable inefficiencies and redundancies from an operational perspective. Finally the power struggles which can occur in silo type structures can actually develop into full scale turf wars, and this can have a very negative impact on the organisation, and can be extremely detrimental to its corporate health (Dobbs et al 2005).

The contemporary view

There is however a growing recognition that a more comprehensive, progressive and proactive approach is now required in order to defend the organisation, and indeed the interests of all the stakeholders. The contemporary view of corporate defence (Lyons 2006) suggests that in the modern era we now have to accept that the corporate world is faced with an ever accelerating rate of change (Furlonger & Barker 2006). This means that knowledge must now be considered to be at best provisional, imperfect or obsolete, as it is subject to change at any point in time. The corporate world is faced with ever-changing and more sophisticated threats, representing an unpredictable world filled with uncertainty and danger (Sull 2006). Under such circumstances the traditional approach to corporate defence is no longer considered to be adequate, and in such an environment a reactive approach is clearly no longer sustainable. We now have to appreciate that defending an organisation includes not only safeguarding and protecting, but also valuing the interests of all of its stakeholders. Consequently this means taking a stakeholder view.

A stakeholder view

By stakeholders I am referring to all parties with a vested interest in the organisation. This includes not only the traditional stakeholders such as the shareholders, but must include clients, business partners and of course our good friends the regulators. Equally, if not more importantly, however are the organisation's line management, and in particular the staff of the organisation; a stakeholder very often neglected. When all our stakeholders' interests are addressed then what you have is what could be described as a happy family. In a happy family there is a shared recognition that all of the members have an important role to play. Each member is aware of their role and is allowed to contribute their fair share. This obviously makes it easier on the rest of the unit; it's called teamwork, where everyone is working towards a common good which will be of benefit to all. An organisation can only operate effectively as a team when there is a sense of unity, trust and mutual respect.

Let us briefly consider stakeholders' interests for a moment. If we think in terms of the broader stakeholder interests then we begin to realise that, yes, there has to be an economic and monetary focus, but we also need to recognise that it is not all about numbers, quarter end figures, and bottom line financials; these don't necessarily resonate with all the stakeholders. To get the required top down and equally important bottom up buy in, we have to look beyond this; we need to ensure that we are selling the organisation's message to all of its stakeholders, including line management and staff. We need to take the stakeholder perspective, where each stakeholder is considered to be an individual, a person, a human being, with human needs and human expectations. Stakeholders need to be considered valued partners within the organisation. We have to realise that stakeholders are also concerned with their health and safety, and their welfare and wellbeing. Corporate defence needs to focus on stakeholders as human beings, as people, not just numbers or bottom line financials. It needs to value the importance of people, and help ensure that their health, safety, welfare and wellbeing are appropriately prioritised. It is only by adopting a 'hearts and minds' approach that an organisation can hope to foster the necessary foundation of trust vital to the establishment of the essential top-down, bottom-up culture required. Obviously from the human perspective corporate defence is therefore an extremely responsible station.

Integrating your defence related functions - a 21st century vision

With this in mind, it seems self evident that corporate defence in the 21st century requires a more eminent role in corporate strategy. It requires a higher priority and profile within the organisation, and a more progressive and proactive approach. It requires a broader stakeholder focus, and a far more comprehensive brief. It requires a strategic re-alignment of defence related activities using both a top-down and bottom-up approach. Ultimately what is needed is a synthesised holistic solution in this area.

So how does an organisation go about addressing all of these issues? All organisations are faced with numerous potential hazards. Examples of these include litigation, fraud, compliance breaches, crime, espionage and natural disasters, to name but a few. These hazards represent not only short term financial risk but knock on reputation risk, not to mention the human implications and costs.

Ultimately all risk has a financial implication, be it on share price or otherwise. These hazards can typically be the result of deficiencies in an organisation's corporate defence program, whereby these deficiencies were either intentionally or unintentionally exploited. Every organisation is faced with its own unique set of risks, threats and vulnerabilities and this will vary depending on corporate culture of the organisation, the business sector it operates in, and its geographic location etc. As a result, each organisation in turn will take its own unique steps to defend against these potential hazards.

The corporate defence domain

In an attempt to safeguard against threats and vulnerabilities most organisations have already introduced a multitude of specialist functions. The corporate defence domain represents these different corporate defence related activities, all of which contribute to the defence of the organisation. Diagram one represents an example of activities which make up what can be described as the corporate defence domain.

A growing number of business analysts and industry experts already acknowledge the critical interdependencies which exist between these activities. Hence the corporate defence domain can be said to represent what can be described as the corporate defence ecosystem, as it relates to the symbiotic relationships which exist between these activities. This relationship highlights the fact that all defence related activities are linked, and that each could be said to represent a link in a chain. Like any chain, it is only as strong as its weakest link, and therefore it could be said that this represents something of an asymmetric challenge for an organisation, as it is the weakest link which is typically exploited. The challenge therefore facing contemporary corporate defence is to unify, align and integrate the management of these defence related activities.

Diagram one



Functional developments in this area

In recent years many forward thinking organisations have already realised this need for change, and at a functional level there has been significant developments in each of these defence related activities. This change has developed into something of an evolutionary process, occurring in gradual phases, and which seems to be occurring in practically all of these activities.

Initially each business unit within an organisation tends to be responsible for developing its own methods in relation to any one of these areas. This represents something of a disparate or fragmented type approach. The area later tends to become consolidated into centralised function, which requires specialist skills. This phase could be described as 1st generation convergence, pulling related issues together under one umbrella, using a centralised type approach. The next phase is a push to embed specialist principles throughout the organisation or on an enterprise-wide basis, as is the case with enterprise risk management etc. There is typically an element of decentralisation involved in this approach. The final phase, what is being described as the integration phase, is now possible as a result of advances which have occurred in technology. This involves moving towards a vertical and horizontal integration of an activity using technology.

These developments are already occurring in practically all of the defence related activities previously referred to. If we stand back a little however, certain observations can be made in relation to these developments. We can see that they are all moving in a similar direction and all are encountering similar challenges. All share a common high level objective, which is to safeguard the organisation. There is however a high degree of duplication and overlap occurring between these activities and an increasingly high level of intersection.

Cross-functional developments

Not only has there been an evolution at a functional level but a similar evolution is now occurring at a cross-functional level. What is now emerging is an evolution in the cross-functional convergence among these activities. This could be referred to as 2nd generation convergence. If we take the example of risk management, we can see that the role of operational risk management (ORM) has been somewhat superseded by enterprise risk management (ERM). There are many reasons for this but primarily it has to do with status and authority within the organisation. Currently, in North America at least, there is a move beyond ERM towards governance, risk and compliance (GRC), which has been described by some as ERM plus the integration of governance and compliance, and by others as the coming together of these three areas (OCEG 2007). On the resilience side, perhaps the concept of business resilience goes even further, as business resilience is viewed in terms of six imperatives, which include risk management, continuity, compliance, security and intelligence (IBM 2004).

This type of cross-functional convergence is also occurring in other defence related activities. If you look at security, at a functional level there is now a move towards a convergence of both physical and logical security which is made possible by advances in technology. Not only that, but compliance, risk management and resilience have also become integral parts of security management. The term enterprise security risk management is one which is currently being used by many professionals involved in security roles (AESRM 2006). At the same time intelligence is also becoming more and more integrated into all of these activities, as organisations recognise that it represents the life blood of any organisation. We are now hearing terms such as enterprise business intelligence (Eckerson & Howson 2005) and indeed risk intelligence (Apgar 2006) more and more. Again it is developments in technology which appear to be facilitating this evolution.

Once again, however, if we stand back a little, we can see that while there have been developments in many of these areas, these tend to illustrate that what has happened is that a number of collective requirements have been identified. These collective requirements appear to be acknowledged as prerequisites for success in practically all of these developments. Generally speaking each of these developments acknowledges that there is a requirement for the each of the following:

- A strategic plan
- An enterprise-wide vision
- A comprehensive strategy
- An alignment of objectives
- A unified management structure
- An adaptable approach

- A cross-functional convergence of complimentary disciplines
- An integration of systems and processes
- A continuous improvement process -An implementation of flexible solutions.

These collective requirements will undoubtedly form the basis for future progress in this area.

Introducing corporate defence management (CDM) as a holistic solution

To help address some of the challenges facing contemporary corporate defence, allow me to introduce the cross-functional discipline of corporate defence management (CDM) which has been defined as (Lyons 2006):

“... the discipline of managing corporate defence in order to adequately defend the interests of the stakeholders. It requires a proactive approach to co-ordinating and integrating a range of interrelated disciplines, which taken together can help to anticipate, prevent, detect and react to potential threats and vulnerabilities, thereby protecting the organisation from potential hazards.”

While CDM is first and foremost a cross-functional discipline, it is also very much a strategic discipline, and could be said to represent a synthesised holistic approach to corporate defence. It represents the consolidation and alignment of defence related activities and helps to ensure that there is a coherent strategic approach in place in relation to corporate defence. It is about helping ensure that all of defence related activities are directed in an integrated strategic manner, and that they are operating in unison towards common objectives. It is about helping to ensure that there is the adoption of similar performance expectations in all these areas, and that they are managed in a co-ordinated and systematic manner. Basically it is about ensuring that all defence related activities are working together as a team, in order to collectively defend the interests of the stakeholders.

The corporate defence cycle

If we now look at what is referred to as the corporate defence cycle (diagram two), we will see that this cycle represents the cornerstones of corporate defence, and addresses the key drivers which should be present in all corporate defence related activities. Namely these four drivers include:

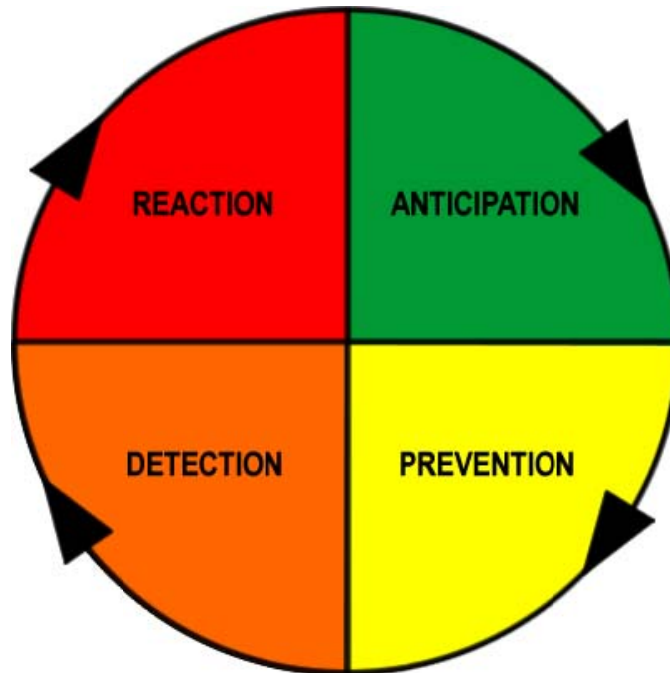
Anticipation: The timely identification and assessment of existing threats and vulnerabilities, and the prediction of future threats and vulnerabilities.

Prevention: Taking sufficient measures to shield the organisation against anticipated threats and vulnerabilities.

Detection: Identification of activity types (exceptions, deviations & anomalies etc) which indicate a breach of corporate defence protocol.

Reaction: The timely response to a particular event or series of events, in order to both mitigate the current situation, and to take further corrective action in relation to deficiencies identified, and to prevent these events re-occurring in the future.

Diagram two: the corporate defence cycle



As can be seen this process is an iterative cycle whereby reaction in turn leads back to anticipation, and so on and so forth. This cycle represents a simple yet effective approach to the challenges facing corporate defence, and for an organisation it represents what has been described as the art and practice of learning. In short this cycle can also help spur constant innovation, reinvention and improvement. However there are certain aspects which need to be fully appreciated. This is not a once off point in time assignment, but rather it is a constantly evolving exercise which is without end. It requires continuous revision and improvement. All those involved in corporate defence related activities must be cognizant of these corporate defence drivers, and they need to be constantly alert to potential threats and vulnerabilities. Finally there needs to be an ongoing level of vigilance present throughout the organisation.

Earlier we looked at defence related activities but each of these activities can also be further subcategorised into various specialist areas, and each of these sub-categories also has an important role to play in defending an organisation. Examples of some of these sub-categories include:

Corporate defence related activities:

| | | |
|--|--|--|
| <p>Corporate governance Directors Remuneration Accountability & audit Relationship with shareholders Corporate responsibility</p> | <p>Risk management Enterprise risk management Operational risk management Credit risk (excluded) Market risk (excluded)</p> | <p>Corporate compliance Regulatory compliance Legal compliance Workplace compliance Internal standards compliance</p> |
| <p>Corporate intelligence BI framework Organisation intelligence Market intelligence Competitive intelligence</p> | <p>Knowledge management Content management Record management Document management Archive management Filing systems</p> | <p>Physical security Security management Premises security People security Operations security Facility security Information security</p> |
| <p>IT security Client security Application security Operating system security Database security Network security Gateway security</p> | <p>Resilience management Emergency operations Crisis management Disaster recovery planning Business contingency planning Business continuity management</p> | <p>Corporate protection Health & safety protection Interruption protection Insurance Receivership / insolvency mgt</p> |
| <p>Corporate controls Internal controls framework Compliance controls Operational controls Financial controls</p> | <p>Corporate assurance Inspection & due diligence Internal & external audit Regulator & rating agencies Standards certification</p> | <p>Corporate investigations Fraud examination Forensic investigation Asset recovery Litigation support</p> |

It should also be appreciated that in the modern era, each of these sub-categories increasingly requires specialist skills and expertise which are essential to their ongoing effectiveness. This table simply gives a further breakdown of the type of defence related activities which organisations need to bring together. It does, however, also indicate the magnitude of the challenge of an enterprise-wide approach towards the alignment and integration of these activities.

The CDM continuum

When we talk about what has been described as the CDM continuum we are referring to the ongoing relationships which exist between these corporate defence related activities. It is for this reason that it was earlier referred to as an ecosystem. This ecosystem refers to their continuous interaction and refers to not only being aware of their dependencies and interdependencies, but also understanding the correlations which exist between these activities. It is about appreciating the cause and effect

nature of these interactions, particularly in terms of potential hazards. It is about considering the possible cascade of consequences which can arise from these interactions, not only direct first order consequences, but indirect second and third order consequences which can occur further down the road. It is for this reason that more and more thought leaders in this field are now referring to the potential dangers which can occur from the ongoing interaction of these multiple risks, resulting in what has referred to as 'Black Swans' (Taleb 2007), being the occurrence of rare events which are potentially devastating to an organisation.

Applying the CDM paradigm

Taking all of the above into account it now seems imperative that we arrive at a change in paradigm in this field. In order to integrate the necessary elements, a three dimensional diagram (diagram three) has been conceived which represents this paradigm change and can help us to conceptualise this integration.

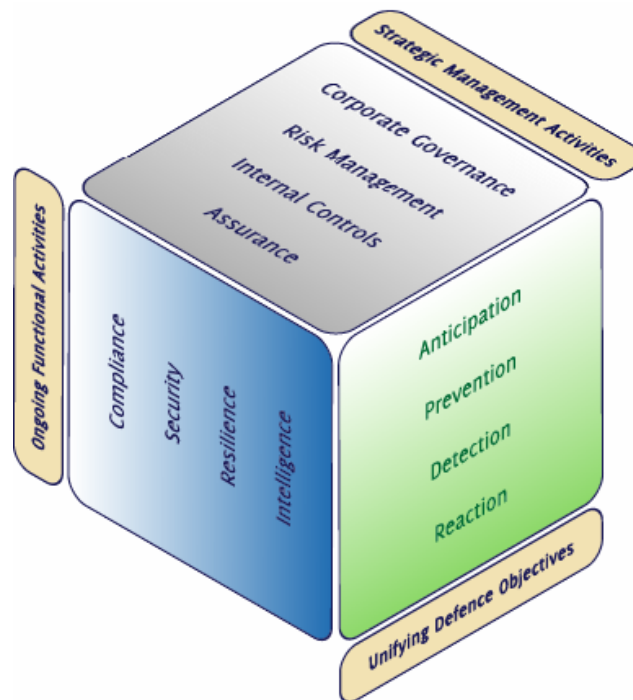


Diagram three: CDM cube

The first dimension on the top of the cube addresses strategic management activities. The second dimension to the front of the cube addresses ongoing functional activities. And finally the third dimension to the right addresses unifying defence objectives.

All of the activities within this paradigm intersect and are intersected by each other. No precise boundaries exist in this diagram in order to help keep away from the traditional silo type mindset. In the modern era each of these defence related disciplines need to be continually cross-referenced against each other.

This paradigm is based on continuing to build on existing structures and frameworks where possible, rather than reinventing yet another new framework.

Strategic management activities: these represent core strategic management areas which correspond with fundamental frameworks and best practices. These activities are based on the four pillars of governance, risk management, controls and assurance (including investigations), and consist of structural frameworks which need to be in place. These activities represent the backbone of corporate defence activities, around which ongoing functional activities operate. Examples of existing frameworks and best practices in these areas include the combined code of corporate governance in the UK, the COSO frameworks for ERM (COSO 2004) and integrated Internal Controls (COSO 1992), and perhaps the IIA's standards of professional practice (IIA 2007) etc.

Ongoing functional activities: these represent essential ongoing operational activities which are required to be continuously operating on an ongoing basis throughout the organisation. They intersect and are intersected by strategic management activities. The core activities include compliance, security (includes physical and IT), resilience (includes business protection) and intelligence (includes knowledge management). There are also a variety of possible frameworks available in these areas, including BS and ISO standards, and COBIT and Basel guidelines etc.

Unifying defence objectives: these relate to the corporate defence cycle referred to earlier. As previously mentioned this cycle operates in a continuous loop and these underlying objectives need to be embedded in the mindset throughout the organisation, and need to be continuously present in day to day activities. The degree to which these objectives are present in the corporate mindset could be said to represent the DNA of corporate defence within the organisation, which will ultimately determine an organisation's robustness. The most robust organisations will have the highest pre-emptive capabilities in place because it is the reaction times to potentially devastating events which will determine the magnitude of the initial impact and the subsequent collateral damage.

The above represented a whistle-stop tour of the changing nature of corporate defence in the 21st century, now it is time to turn our attention to business continuity and resilience.

The emergence of enterprise resilience and collaborative resiliency

In recent times we have seen the emergence of the term enterprise resilience (Sheffi 2005), which in its simplest form could be said to refer to an organisation's ability to withstand, rebound or recover from a shock, disturbance or disruption. Over the years we have seen most organisations move away from the reactive 'seat of the pants' approach, so often associated with emergency operations and crisis management, towards a more positive approach requiring a certain degree of planning in advance. Initially disaster recovery planning simply addressed low probability, high impact, physical events, which more often than not required relocation to a hot-site. However this later developed into more detailed contingency planning, which began to address higher probability, lower impact events, which could also be addressed in-house. The introduction of a more proactive approach, with a business performance focus, came in the form of business continuity management, whereby the potential added value of this discipline began to be recognised. Finally, resilience management has come to represent a somewhat more holistic approach to the challenge of operational resilience.

If we now revisit the CDM paradigm, a number of issues become apparent. This paradigm should be seen as representing an organisation's toolkit, whereby each element is considered a valuable component in a well run organisation. Each of these activities requires that the other elements are operating effectively. As an example, purely from a resilience perspective, we can see that there are requirements in each of these areas. There has to be governance, risk management, control and

assurance structures in place in order to actively manage resilience strategy. Systems, processes and procedures need to be operating to ensure ongoing compliance, security and communication of intelligence. Those involved in resilience need to be constantly focused on anticipating, preventing, detecting and reacting to issues which could have an impact on the organisation's performance, and also to help promote continuous improvement.

The same is also true of the other activities, and each of these also requires a resilience focus in their own performance, which could be described as a collaborative approach to resiliency. So we can now see that not only are these activities generally present as functions or disciplines within an organisation, but increasingly each one of these elements is actually required to be an integral part of each one of these individual disciplines. Therefore it is apparent that there is now a growing appreciation of the need for cross-functional expertise throughout the organisation, and in this regard it has been said that perhaps we are only now beginning to see the forest from the trees in this area.

Business continuity opportunities

So, now we finally arrive at the opportunities which exist for those involved in business continuity initiatives. Based on what we have seen so far it has to be said that from a corporate defence perspective at least, those involved in business continuity are already at the forefront of developments in the management of corporate defence. And they are well positioned to play a leading role in corporate defence developments in the future. They have already gained valuable integration and convergence experience, as business continuity already focuses on key business concerns on an enterprise-wide basis, and they should already possess a strategic enterprise-wide view. They also possess a strategic advantage over other components, as resilience must be considered a primary feature of any organisation's mission statement. The challenge however facing business continuity exponents is to raise its profile and status within the organisation.

For those involved in business continuity and resilience management, a number of opportunities present themselves. First and foremost there is an opportunity to be a key player in corporate defence within your organisation, given the experience and positioning referred to previously. This however could take a number of forms. There is the opportunity to simply promote business continuity goals and objectives within the broader corporate defence agenda. There is the opportunity for business continuity to further integrate with some of the other defence components. Ultimately however there is the opportunity to take a lead role on corporate defence, to actually be the driving force behind corporate defence within your organisation, rather than simply allowing one of the other defence related disciplines to take the initiative in this area, and merely falling into line.

Conclusion

In summary, while business continuity as it currently stands represents an important step in corporate defence, it is an area that itself is continually evolving and has not yet reached its final destination. It is already developing in the direction of an even broader cross-functional discipline such as CDM. Whether those involved in business continuity will successfully exploit the opportunities presenting themselves in corporate defence remains to be seen. One thing however seems certain, if it is not those involved in business continuity then it will be those from within other defence related disciplines, for that is the nature of progress. Finally, it is important to remember that opportunities exist only for

those with both the ability to see them and to actually act upon them; for that is, as they say, the nature of evolution.

References

- Apgar, D (2006) *Risk Intelligence: Learning to Manage What We Don't Know*, HBS Press 2006
- Dobbs, R, Leslie, K, & Mendonca, L (2005) *Building the Healthy Corporation*, The McKinsey Quarterly 2005 No. 3, [Online], Available: <http://www.mckinseyquarterly.com>
- Furlonger, D & Barker, JA (2006) *The Risk of Uncertainty: Implications for the Future*, Webcast, [Online], Available: <http://www.bettermanagement.com> [1 Aug 2006] IBM (2004),
- Business Resilience: *Proactive Measures for Forward Looking Enterprises*, [Online], Available: <http://www.ibm.com>
- Lyons, S (2006) *Corporate Defence: Are Stakeholders Interests Adequately Defended* The Journal of Operational Risk, Volume 1, No. 2, Summer 2006, pp. 67-73 Lyons, S (2006)
- An Executive Guide to Corporate Defence Management*, [Online], Available: <http://www.grc-usa.com>
- Sheffi, Y (2005) *The Resilient Enterprise: Overcoming Vulnerability For Competitive Advantage*, MIT Press 2005
- Sull, D (2006) *How to Manage in an Unpredictable World*, Online video course, [Online], Available: <http://www.news.ft.com>
- Taleb, N (2007) *The Black Swan*, Penguin Books Ltd 2007
- The Alliance of Enterprise Security Risk Management (AESRM)* (2006), [Online], Available: <http://www.aesrm.org>
- The Committee of Sponsoring Organizations of the Treadway Commission (2004) *Enterprise Risk Management – Integrated Framework*, (Sept 2004), [Online], Available: <http://www.coso.org>
- The Committee of Sponsoring Organizations of the Treadway Commission (1992) *Internal Control – Integrated Framework*, (1992), [Online], Available: <http://www.coso.org>
- Eckerson, W & Howson, C (2005) *Enterprise Business Intelligence: Strategies and Technologies for Deploying BI on an Enterprise Scale* (Aug 2005),
- The Data Warehousing Institute (TDWI)*, [Online], Available: <http://www.tdwi.org>
- The Financial Services Authority (2003) *The Combined Code on Corporate Governance*, (July 2003), [Online], Available: <http://www.fsa.gov.uk>
- The Institute of Internal Audit (2007) *International Standards for the Professional Practice of Internal Auditing* (Jan 2007), [Online], Available: <http://www.theiia.org>
- The Open Compliance and Ethics Group (OCEG) (2007), *The GRC Illustrated Series* [Online], Available: <http://www.oceg.org>