Risk Management's Role in Corporate Defense

Sean Lyons[*]

[*] Risk-Intelligence-Security-Control (RISC) International (Ireland). sean.lyons@riscinternational, i.e.: www.riscinternational.ie/

1. What Does Corporate Defense Mean in Your Organization?

Although the term corporate defense may be somewhat intuitively understood, its precise meaning can vary from individual to individual, and as a result its priority (both from organization to organization, and indeed within an organization) can also vary. Its precise definition can therefore vary depending on the circumstances in which it is applied. Examples of activities which use this term include areas such as legal, security, resilience, compliance, audit and, of course, risk management. Each of these activities shares the common high level objective of attempting to defend the organization, and could be said to represent different lines of defense. For the time being let us consider corporate defense as representing an organization's program for self defense or self-protection. By program of self defense we are of course referring to the structures, measures, mechanisms and processes in place within an organization that are aimed at defending the interests of all of its stakeholders. Stakeholders refer to all parties with a vested interest in the organization; this includes not only the traditional stakeholders such as the shareholders, but must include clients, business partners and of course the regulators. Equally importantly, however, is the organization's line management, and in particular the staff of the organization, a stakeholder very often neglected. Managing corporate defense is therefore an extremely responsible station, as it involves the responsibility for adequately defending the interests of all of the stakeholders of an organization, both in terms of monetary and human implications.

2. The Traditional View

The traditional view of corporate defense, which focuses on security and litigation issues, unfortunately represents a very narrow view and restricted focus. The traditional mind-set is generally one of a reactionary nature, where corporate defense issues only appear on the radar after a serious incident has occurred, which very often has 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 organization with a traditional view of corporate defense, defense-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; rather they can very often be the subject of internal power struggles. As a consequence of this type of traditional mind-set, an organization can be subject to typically negative impacts. Generally this type of attitude can result in an organization operating in a crisis management mode, whereby it finds itself continuously firefighting on a daily basis. Very often the overall responsibility and accountability for corporate defense are dispersed or fragmented, diluted or ambiguous. In certain scenarios they can sometimes even be nonexistent. This can obviously result in omissions or gaps, and these in turn create vulnerabilities that can later be exploited, rendering many other related efforts ineffective in the process. All of the intersection, duplication and overlap of activities that can occur in the silo-type environment can also result in considerable inefficiencies and redundancies from an operational perspective. Finally, the power struggles that can occur in silo-type structures can actually develop into full-scale turf wars. This can have a very negative impact on the organization, and can be extremely detrimental to its corporate health (Dobbs et al., 2005).

3. The Contemporary View

In the 21st century, contemporary corporate defense has in fact a far more comprehensive brief, and there is now a growing recognition that a more progressive and proactive approach is required in order to defend the organization, and indeed the interests of all the stakeholders. The contemporary view of corporate defense (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 and 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 defense 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 organization includes not only safeguarding and protecting, but also valuing the interests of all of its stakeholders. Consequently this means taking a stakeholder view.

4. A Stakeholder View

Let us briefly consider stakeholders' interests for a moment**.** If we think in terms of the broader stakeholder interests, then we begin to realize that there has to be an economic and monetary focus, but we also need to recognize 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 organization'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 organization. We have to realize that stakeholders are also concerned with their health, safety, welfare and well-being. Corporate defense 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 well-being are appropriately prioritized. It is only by adopting a "hearts and minds" approach that an organization can hope to foster the necessary foundation of trust vital to the establishment of the essential top-down, bottom-up culture required.

When all the stakeholders' interests are addressed, you have 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 his role and is allowed to contribute his 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 that will be of benefit to all. An organization can only operate effectively as a team when there is a sense of unity, trust and mutual respect.

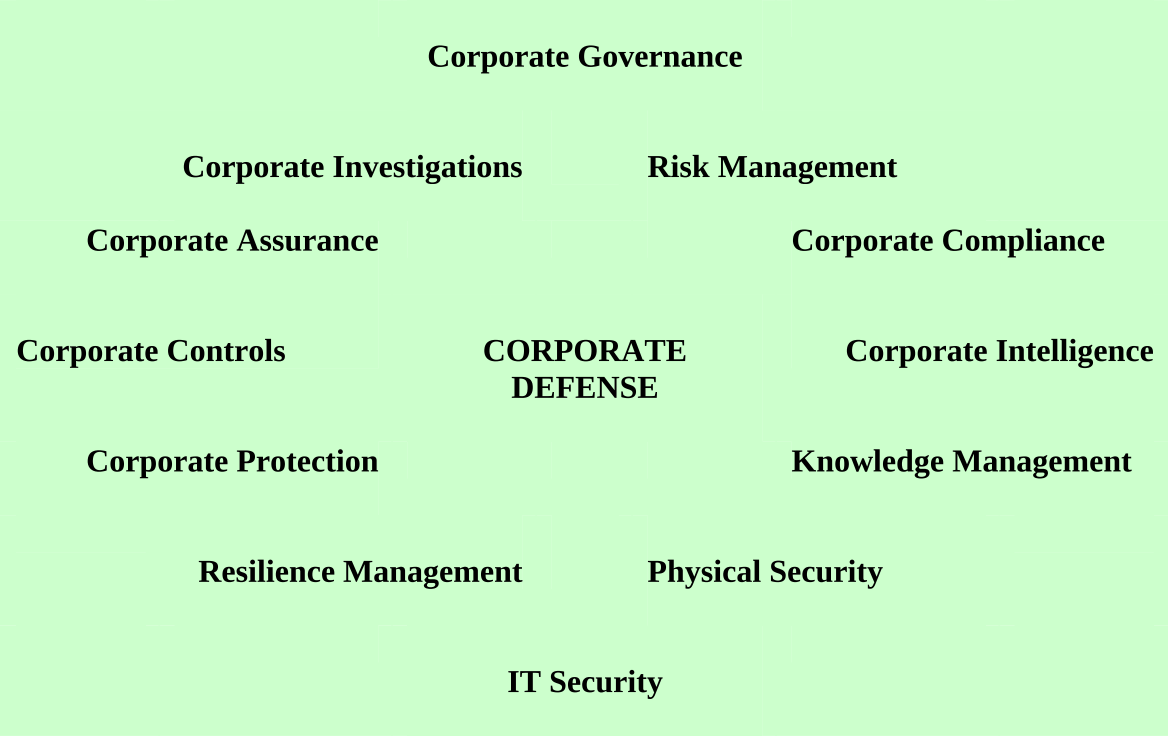
5. Integrating Your Defense-Related Functions: A 21st Century Vision

With this in mind, it seems self-evident that corporate defense in the 21st century requires a more eminent role in corporate strategy. It requires a higher priority and profile within the organization, 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 defense-related activities using both a top-down and bottom-up approach. Ultimately what is needed is a synthesized holistic solution in this area.

So how does an organization go about addressing all of these issues? All organizations are faced with numerous potential hazards. Examples of these potential hazards 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. The occurrence of these hazards can typically be the result of deficiencies in an organization's corporate defense program, whereby these deficiencies were either intentionally or unintentionally exploited. Every organization is faced with its own unique set of risks, threats and vulnerabilities, and this will vary depending on corporate culture of the organization, the business sector it operates in, its geographic location, etc. As a result, each organization in turn will take its own unique steps to defend against these potential hazards.

6. The Corporate Defense Domain

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



A growing number of business analysts and industry experts already acknowledge the critical interdependencies that exist between these activities. Hence the corporate defense domain can be said to represent what can be described as the corporate defense ecosystem, as it relates to the symbiotic relationships that exist between these activities. This relationship highlights the fact that all defense-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 organization, as it is the weakest link that is typically exploited. The challenge therefore facing contemporary corporate defense is to unify, align and integrate the management of these defense-related activities.

7. Functional Developments in This Area

In recent years many forward-thinking organizations have already realized this need for change. At a functional level, there have been significant developments in each of these defense-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 organization 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 a centralized function, which requires specialist skills. This phase could be described as first generation convergence, pulling related issues together under one umbrella, using a centralized-type approach. The next phase is a push to embed specialist principles throughout the organization or on an enterprise-wide basis, as is the case with enterprise risk management, etc. There is typically an element of decentralization involved in this approach. The final phase, what is being described as the integration phase, is now possible as a result of advances that have occurred in technology. This involves moving towards a vertical and horizontal integration of an activity using technology. While this evolution is occurring in practically all of these activities, we will use the example of risk management here to help illustrate the point.

7.1 The Disparate Phase: Ad-hoc Risk Management

Over the years, many organizations allowed individual business units within their organization to develop their own approach to the management of risk. These approaches were often developed on an inconsistent basis, the result being that risk management across the business units was generally unsystematic and unstructured.

7.2 The Centralized Phase: Centralized Risk Management Functions

In order to help develop a more consistent approach, many organizations introduced specific centralized risk management functions. These risk management functions had responsibility for managing business risks from a centralized source. This included credit, market and later operational risk functions. The introduction of “operational risk management” (ORM) as a discipline for the first time represented formal recognition of the requirement to manage risks other than market and credit risks.

7.3 The Enterprise-wide Phase: Enterprise Risk Management (ERM)

The development of the “enterprise risk management” (ERM) framework was designed to help embed risk management principles and processes throughout the entire enterprise. This promotion of a risk management culture was an attempt to help ensure that all areas within the organization would adopt a risk-based approach and systematically focus on the identification, measurement and management of risks.

7.4 The Integrated Phase: Integrated Risk Management

Over time, however, many organizations have unintentionally created risk management “silos,” which in turn have created difficulties in the management of risk at strategic, tactical and operational levels. These difficulties have however led organizations to recognize the necessity to integrate these silos. Responding to business needs, leading vendors are now developing and providing end-to-end risk management solutions that consist of integrated suites running on common application services and platforms.

As more and more organizations appreciate that risk management represents a core process in an organization, risk management is becoming more and more integrated into all of the other defense-related activities. Similar developments are also occurring in practically all of the defense-related activities represented in the corporate defense domain. If we stand back a little, however, certain observations can be made in relation to these functional developments. We can see that they are all moving in a similar direction and are all encountering similar challenges. All share a common high level objective, which is to safeguard their organization. However, there is also a high degree of duplication and overlap occurring between these activities, and an increasingly high level of intersection.

8. 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 look at “compliance management” as an example, we can see that in recent years compliance (perhaps regulatory compliance in particular) has become a serious corporate concern and has been elevated to the top end of most organizations’ priority lists. This has seen compliance management increasingly impact all aspects of the enterprise, and we are also seeing the introduction of integrated compliance management technology in many organizations. In North America in particular there is now a move beyond compliance management towards “governance, risk and compliance” (GRC), which has been described by some as compliance management plus the integration of governance and risk management, 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 now viewed not only as “business continuity and disaster recovery” (BCDR), but increasingly in terms of a number of other imperatives, which not only include BCDR but also encompass compliance and risk management as well as security and intelligence perspectives (IBM, 2004).

This type of cross-functional convergence is also occurring in other defense-related activities. If we look at security, at a functional level there is now a move towards a convergence of both physical and logical security that 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 a term 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 organizations recognize that it represents the lifeblood of any organization. We are now hearing terms such as "enterprise business intelligence" (Eckerson and Howson, 2005) and indeed "risk intelligence" (Apgar, 2006) more and more. Again, developments in technology 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 developments 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 each of the following:

- A strategic plan
- A comprehensive strategy
- A unified management structure
- A convergence of complementary disciplines
- A continuous improvement process
- An enterprise-wide vision
- An alignment of objectives
- An adaptable approach
- An integration of systems and processes
- An implementation of flexible solutions

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

9. Introducing Corporate Defense Management (CDM) as a Holistic Solution

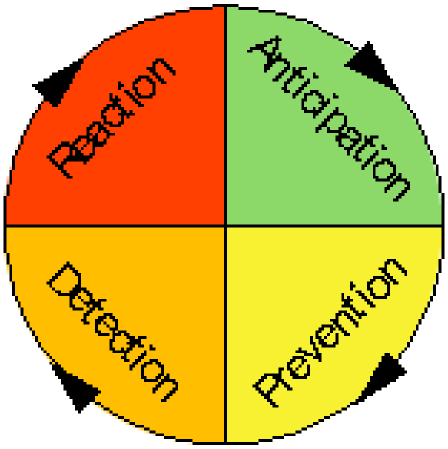
To help address some of the challenges facing contemporary corporate defense, allow me to introduce the cross-functional discipline of "corporate defense management" (CDM), which has been defined as (Lyons, 2006):

> *… the discipline of managing corporate defense in order to adequately defend the interests of the stakeholders. It requires a proactive approach to coordinating 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 organization 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 synthesized holistic approach to corporate defense. It represents the consolidation and alignment of defense-related activities and helps to ensure that there is a coherent strategic approach in place in relation to corporate defense. It is about helping ensure that all defense-related activities are directed in an integrated strategic manner, and that they are operating in unison toward 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 coordinated and systematic manner. Basically it is about ensuring that all defense-related activities are working together as a team, in order to collectively defend the interests of the stakeholders.

10. The Corporate Defense Cycle

If we now look at what is referred to as the corporate defense cycle, we will see that this cycle represents the cornerstones of corporate defense and addresses the key drivers that should be present in all corporate-defense-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 organization against anticipated threats and vulnerabilities.
Detection: Identification of activity types (exceptions, deviations & anomalies, etc.), which indicate a breach of corporate defense protocol.
Reaction: The timely response to a particular event or series of events, in order to both mitigate the current situation, to take further corrective action in relation to deficiencies identified and to prevent these events re-occurring in the future.

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 defense, and for an organization 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 that need to be fully appreciated. This is not a once-off point in time assignment, but rather it is a constantly evolving exercise that is without end. It requires continuous revision and improvement. All those involved in corporate-defense-related activities must be cognizant of these corporate defense 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 organization.

Earlier in the corporate defense domain, we looked at examples of defense-related activities, but each of these activities can also be further subcategorized into various specialist areas, and each of these sub-categories also has an extremely important role to play in defending an organization. It should also be appreciated that in the modern era, each of these sub-categories increasingly requires specialist skills and expertise that are essential to their ongoing effectiveness**.** The table below simply gives a further breakdown of the types of defense-related activities that organizations need to bring together. While this table should not be considered to be a complete listing of defense-related activities, it does give an indication of the magnitude of the challenge of an enterprise-wide approach towards the alignment and integration of these activities. Examples of some of these sub-categories include:

Corporate-Defense-Related Activities

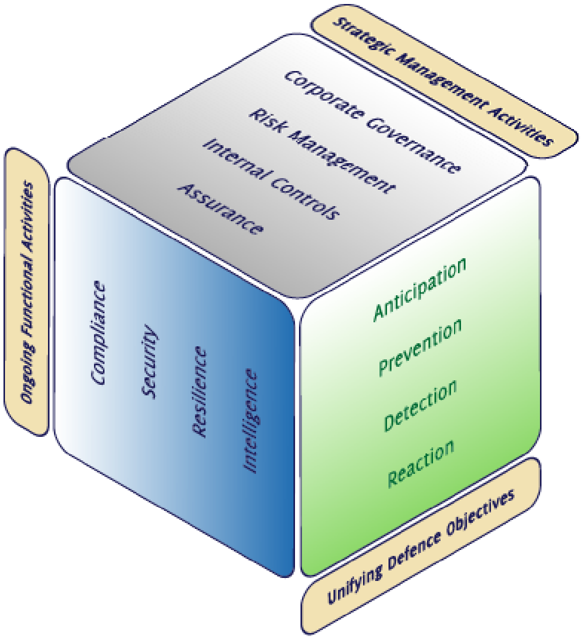
Corporate Governance • Directors • Remuneration • Accountability & Audit • Relationship with Shareholders • Corporate Responsibility	**Risk Management** • Enterprise Risk Management • Operational Risk Management • Credit Risk (excluded) • Market Risk (excluded)	**Corporate Compliance** • Regulatory Compliance • Legal Compliance • Workplace Compliance • Internal Standards Compliance
Corporate Intelligence • BI Framework • Organization Intelligence • Market Intelligence • Competitive Intelligence	**Knowledge Management** • Content Management • Record Management • Document Management • Archive Management • Filing systems	**Physical Security** • Security Management • Premises Security • People Security • Operations Security • Facility Security • Information Security
IT Security • Client Security • Application Security • Operating System Security • Database Security • Network Security • Gateway Security	**Resilience Management** • Emergency Operations • Crisis Management • Disaster Recovery Planning • Business Contingency Planning • Business Continuity Management	**Corporate Protection** • Health & Safety Protection • Interruption Protection • Insurance • Receivership/Insolvency Management
Corporate Controls • Internal Controls Framework • Compliance Controls • Operational Controls • Financial Controls	**Corporate Assurance** • Inspection & Due Diligence • Internal & External Audit • Regulator & Rating Agencies • Standards Certification	**Corporate Investigations** • Fraud Examination • Forensic Investigation • Asset Recovery • Litigation Support

11. The CDM Continuum

When we talk about what has been described as the "CDM Continuum," we are referring to the ongoing relationships that exist between these corporate-defense-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 that 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 that can arise from these interactions, not only direct first order consequences, but indirect second and third order consequences that 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 that can occur from the ongoing interaction of these multiple risks, resulting in what have been referred to as "Black Swans" (Taleb, 2007), being the occurrence of rare events that are potentially devastating to an organization.

12. 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 has been conceived that represents this paradigm change and can help us to conceptualize this integration.



The first dimension 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 defense 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 mind-set. In the modern era each of these defense-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.

<u>Strategic Management Activities</u>: These represent core strategic management areas that 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 that need to be in place. These activities represent the backbone of corporate defense 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 United Kingdom (FSA, 2003), the COSO frameworks for ERM (COSO, 2004), 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 that are required to be continuously operating on an ongoing basis throughout the organization. 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, COBIT and Basel guidelines, etc.

Unifying Defense Objectives: These relate to the corporate defense cycle referred to earlier. This cycle operates in a continuous loop, and these underlying objectives need to be embedded in the mind-set throughout the organization, and need to be continuously present in day-to-day activities. The degree to which these objectives are present in the corporate mind-set could be said to represent the DNA of corporate defense within the organization, which will ultimately determine an organization's robustness. The most robust organizations will have the highest pre-emptive capabilities in place, because the reaction times to potentially devastating events 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 defense in the 21st century; now it is time to turn our attention specifically to risk management.

13. Developments in Risk Management

Initially the focus of risk management attention was not on operational risk but primarily focused on business issues such as market and credit risks, with operational risk as somewhat of an afterthought. Operational risk therefore was seen to represent any risk not categorized as market or credit risk. The arrival of ORM as a discipline was seen as a major breakthrough and was perhaps the most significant development in the evolution of contemporary corporate defense. ORM focused attention on the existence of operational risks and addressing these risks in a disciplined and systematic manner. It represented official recognition of the need to address operational risks in a formal way, rather than in the ad-hoc manner that had previously been employed. From a corporate defense perspective, however, critics of ORM believe that it is not fulfilling its defensive responsibilities, as very often (with the spotlight on Basel II, etc.) the focus of ORM functions is overly concerned with issues such as capital adequacy allocation requirements and the development of complex quantitative financial models. In many cases, as a discipline, ORM lacks sufficient status within the organization in order to be effective. It is often viewed as having an inferior status, being considered a subordinate within the extended risk family, and is thus treated as somehow deserving of a lower priority than that of market or credit risk.

The emergence of ERM in many organizations has meant that the role of ORM has been somewhat superseded and further undermined. There are many reasons for this, but primarily it has to do with status and authority within the organization. Many providers of ERM solutions are now excluding financial risk (market and credit risk) and offer solutions to which focus not only operational risk but also compliance risk, technology risk and strategic risk. As noted above, these risks were previously considered to reside under the umbrella of operational risk. While its enterprise-wide contribution to corporate defense certainly cannot be denied, critics of ERM believe that from a corporate defense perspective, focusing solely on risk as a theoretical quantitative measure is often somewhat abstract and ultimately too narrow a view. There are claims that it is not sufficiently practical to adequately address the immediate impact of the ongoing and continuous nature of day-to-day threats and vulnerabilities. It is also argued that sufficient attention is not being focused on the human aspect within the organization, and that the welfare, safety and well-being of individuals as human beings cannot be measured in purely quantitative terms. Quantification models and techniques very often only measure the possible financial impact of direct first order implications, while ignoring the cascade of consequences that can follow and that can result in second and third order implications, which can negatively impact on not only the firm's reputation risk but ultimately the market value of the organization itself. The end result has been that although many organizations have embraced ERM, a disconnect has been developing that needs to be addressed.

If we now revisit the CDM paradigm, a number of issues become apparent. This paradigm should be seen as representing an organization's toolkit, whereby each element is considered a valuable component. Each of these elements requires that the other elements are operating effectively. As an example, from a risk management perspective, we can see that there are requirements in each of these elements. There has to be governance, control and assurance structures in place in order to actively manage risk strategy. Systems, processes and procedures need to be operating to ensure that compliance, security and resilience risks are mitigated, and the communication of risk intelligence is paramount. Those involved in risk management need to be constantly focused on anticipating, preventing, detecting and reacting to issues that could have an impact on the organization'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 risk management focus in their own performance, which could be described as a collaborative approach to risk management. So we can now see that not only are these defense activities generally present as functions or disciplines within an organization, 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 organization, 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.

14. Risk Management Opportunities

We finally arrive at the opportunities that exist for those involved in risk management initiatives. Based on what we have seen so far, it has to be said that from a corporate defense perspective at least, those involved in risk management are already at the forefront of developments in the management of corporate defense. And they are well positioned to play a leading role in corporate defense developments in the future. They have already gained valuable integration and convergence experience, as risk management already focuses on key business risks 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 risk appetite (the risk and reward relationship) must be considered a primary feature of any organization's mission statement. The primary challenge facing those involved in risk management is to bridge the disconnection that has developed between not only the human aspect of risk management but also the growing disconnect between risk management and the ongoing, on the ground, day-to-day functional activities and operations.

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

15. Conclusion

In summary, while risk management as it currently stands represents an important step in corporate defense, 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 risk management will successfully exploit the opportunities presenting themselves in corporate defense remains to be seen. One thing, however, seems certain, if it is not those involved in risk management then it will be those from within other defense-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*. Boston: Harvard Business School Press.

Dobbs, R., Leslie, K., and Mendonca, L. 2005. "Building the Healthy Corporation." The McKinsey Quarterly, No. 3. [Online]. Available: http://www.mckinseyquarterly.com

Eckerson, W., and Howson, C. 2005. "Enterprise Business Intelligence: Strategies and Technologies for Deploying BI on an Enterprise Scale." The Date Warehousing Institute (TDWI), Aug. [Online]. Available: http://www.tdwi.org

Furlonger, D., and Barker, J.A. 2006. "The Risk of Uncertainty: Implications for the Future." Webcast, Aug. 1. [Online]. Available: http://www.bettermanagement.com.

IBM. 2004. "Business Resilience: Proactive Measures for Forward Looking Enterprises." [Online]. Available: http://www.ibm.com.

Lyons, S. 2006. "Corporate Defense: Are Stakeholders Interests Adequately Defended?" The Journal of Operational Risk 1(2): 67–73.

_______. 2006. "An Executive Guide to Corporate Defense Management." [Online]. Available: http://www.grc-usa.com.

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*. London: Penguin Books.

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. [Online]. Available: http://www.coso.org.

The Committee of Sponsoring Organizations of the Treadway Commission. 1992. "Internal Control—Integrated Framework." [Online]. Available: http://www.coso.org.

The Financial Services Authority. 2003. The Combined Code on Corporate Governance. July. [Online]. Available: http://www.fsa.gov.uk.

The Institute of Internal Audit. 2007. International Standards for the Professional Practice of Internal Auditing. Jan. [Online]. Available: http://www.theiia.org.

The Open Compliance and Ethics Group (OCEG). 2007. The GRC Illustrated Series. [Online]. Available: http://www.oceg.org.