

An Introduction To Corporate Defense Management (CDM)

Contemporary corporate defense explained

While corporate defense is a term quite often used and perhaps intuitively recognized, it remains somewhat of a mystery as to why to date it has not occupied a more eminent role in corporate strategy. It appears that its role and purpose are not fully understood or indeed its worth fully appreciated. All too often it is considered in a very narrow focus, as discussions on the topic will very often be restricted to corporate legal or security issues. Contemporary corporate defense has of course a far more comprehensive brief.

“Corporate Defense can be defined as an alchemy of both science and art, aimed at defending an organization from a multitude of possible threats and vulnerabilities.”¹

Defending an organization includes defending the company name and all its stakeholders. This includes defending the shareholders, the business partners, and of course its clients. Defending the company name also means defending its people, management and staff. Consequently the defense of the organization is an extremely responsible station.

The critical questions which must be raised are obvious ones, where exactly does the responsibility for corporate defense actually rest within the organization and who is accountable? The challenge of defending against threats and vulnerabilities is without end, it is a constantly evolving process which requires ongoing vigilance in order to ensure continuous improvement. It requires a strategic outlook and the alignment of a number of existing disciplines which need to be coordinated in a strategic manner.

Organizations already implement a variety of what could be described as corporate defense related disciplines. Each of these represents an important link in the chain to help corporations defend against internal and external threats. Unfortunately very often these disciplines are not in alignment with one another and tend to operate in isolation (e.g. in silos) thereby creating vulnerability, and reducing their potential for overall effectiveness. In order to achieve a holistic solution to corporate defense, the symbiotic relationship which exists between these disciplines must be understood and fully appreciated. For corporate defense strategies to be effective they must incorporate all of these disciplines in a coordinated and systematic manner. What needs to be created is a cybernetic loop whereby communication includes multi-dimensional feedback, operating vertically (both top-down and bottom-up) as well as horizontally.

Corporate Defense Management (CDM) as a strategic discipline

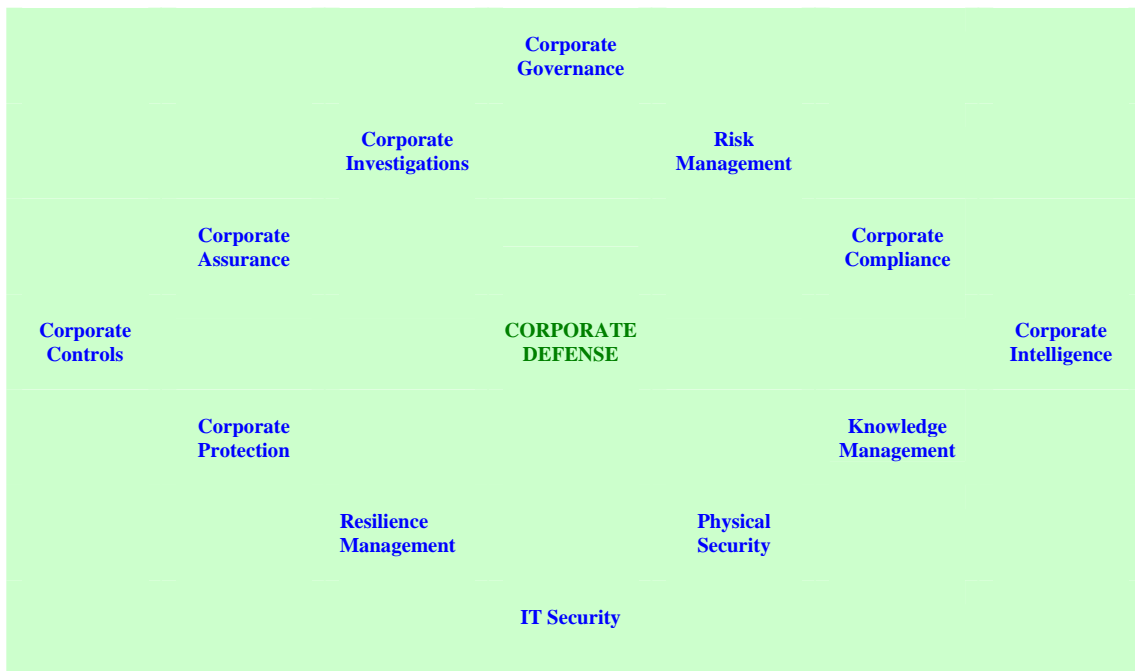
The necessary holistic approach needed must not only include Front, Middle and Back office participation, but also requires an independent critical role with high level responsibility for strategy and planning, co-ordination, and crucially, communication. It is time to introduce a mechanism to proactively manage these challenges, and Corporate

¹Corporate Defence: Are Stakeholders Interests Adequately Defended? – Sean Lyons – The Journal of Operational Risk, Vol. 1, No. 2 (www.thejournalofoperationalrisk.com)

Defense Management (CDM) represents a holistic solution to the challenges facing corporate defense.

CDM can be defined as *“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.”*²

The Corporate Defense Domain



The function of CDM should be responsible for directing and coordinating the range of related defensive disciplines in order to achieve a coherent strategic approach. For corporate defense related disciplines, their defensive mission is generally to anticipate, prevent, detect and react to potential threats and vulnerabilities in a timely manner. Therefore it could be said that anticipation, prevention, detection and reaction are the four cornerstones of a corporate defense

- **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.

² Corporate Defence Management: A Strategic Imperative – Sean Lyons – BankDirector.com / Resource Center / Strategy - Oct 2006 (www.bankdirector.com)

- **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.

The task of CDM involves the consolidation of the all defensive activities, which involves the convergence and alignment of a multitude of diverse yet interrelated domains. CDM must be all inclusive in order to be effective, with all defensive disciplines functioning in unison. This holistic approach must include input and co-operation from Front, Middle and Back Office activities. Using advanced technologies it is now possible to create a fusion of these disciplines and to eliminate any possible “Chinese walls”. This task demands a spirit of co-operation from all parties, to help facilitate working together in a positive and proactive manner. This is easiest achieved by utilizing existing structures and relationships where possible.

Leveraging from related best practice frameworks

In order to adequately defend stakeholder interests, there must first be an appropriate structure in place to help maximize the possibility of achieving this objective. This structure will act as the foundation on which a successful corporate defense program can be built and the framework for interaction with other related disciplines.

Organizations already have a variety of structures in place which intersect each other in numerous ways and on multiple levels.

- | | | |
|------------------|------------------|---------------|
| - Parent Company | - Business Units | - Departments |
| - Subsidiaries | - Divisions | - Branches |

A number of best practice guidelines exist in relation to frameworks in the core strategic management areas of corporate defense. The implementation of these best practices helps to assist in the achievement of the organizations objectives. CDM ideally should position itself in such a way that these related disciplines feed into the corporate defense process rather than creating yet another complex framework. The challenge for CDM is to align itself to these existing frameworks and harness these synergies in a constructive way, while also adding its own unique value in the process.

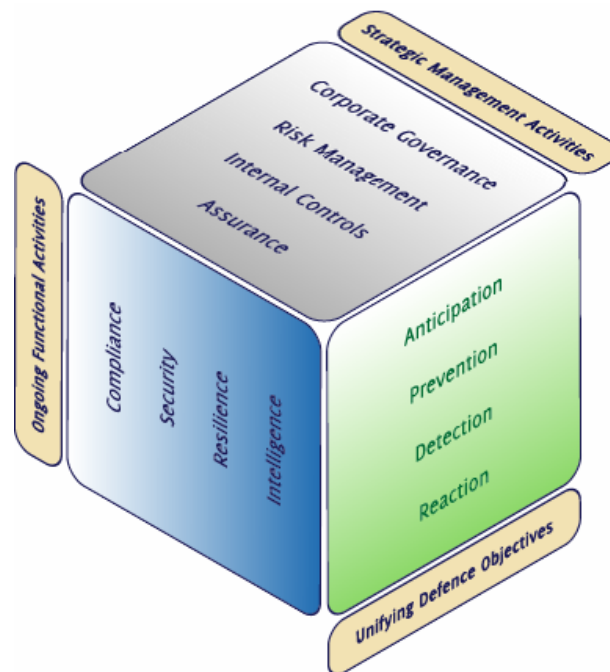
The CDM Paradigm

To this end a CDM paradigm has been conceived to help integrate the necessary elements. By utilizing existing components this paradigm presents a conceptual structure which allows for the application, understanding, implementation and cohesive integration of these existing components. This new paradigm³ is based on a three dimensional view of corporate defense. The three dimensions are outlined as follows:

- Strategic Management Activities
- Ongoing Functional Activities
- Unifying Defense Objectives

³ An Executive Guide To Corporate Defence Management (CDM) – Whitepaper - Sean Lyons – (www.riskcenter.com)

The CDM Paradigm



Strategic Management Activities

The 1st dimension relates to certain strategic management activities. In relation to CDM certain areas are considered to be the core strategic management areas. These relate to frameworks and best practices which should form the backbone of the organization's corporate defense strategic activities, around which other related functional disciplines operate. These core areas relate to the following four pillars:

- Corporate Governance⁴
- Risk Management⁵
- Internal Controls⁶
- Assurance (includes Investigations)⁷

Each of these corporate defense pillars are considered to be fundamental strategic frameworks which are required to be operating effectively in order to successfully implement a robust corporate defense program. The critical frameworks put in place to enable the operation of each of these pillars, will in turn determine the operational effectiveness of other ongoing functional activities, which for the purposes of corporate defense are regarded as the 2nd dimension in the paradigm.

Ongoing Functional Activities

The 2nd dimension focuses on essential ongoing functional activities. A number of these operational activities are considered to be the key functional areas within corporate

⁴ See "The Combined Code on Corporate Governance" – July 2003 – www.fsa.gov.uk

⁵ See "Enterprise Risk Management – Integrated Framework" – Sept 2004 - www.coso.org

⁶ See "Internal Control – Integrated Framework" – 1992 – www.coso.org

⁷ See "International Standards For the Professional Practice of Internal Auditing" – Jan 2004 - www.theiia.org

defense, in so much as they are required to be continuously operating on an ongoing basis throughout the organization. These activities both intersect and are intersected by strategic management activities and are considered to be essential in the implementation of a robust program. The four core activities relate to the following:

- Compliance
- Security (includes Physical and IT)
- Resilience (includes Protection)
- Intelligence (includes Knowledge Management)

As a multitude of best practice frameworks, bench marks and guidelines are available in these areas, and the appropriate “best fit” should be considered in consultation with both in-house and external professionals in the related areas. These core ongoing functional activities generally have a number of somewhat specialist disciplines operating within their sphere of activity. The requirement for specialist disciplines is increasing constantly as more and more complicated and sophisticated techniques are required to keep pace with technological progress. The interaction between these disciplines and the reporting and communication lines in place will determine the robustness of the organization’s defensive capabilities. Each of these specialist disciplines is in itself considered to be a valuable link in the corporate defense chain, and in turn weaknesses or vulnerabilities in one area can have a potentially damaging impact elsewhere within the organization. The old maxim that “the chain is only as strong as its weakest link” certainly applies.

Unifying Defense Objectives

The 3rd dimension focuses on what are termed unifying defense objectives. From a corporate defense perspective the underlying objectives which must be continuously present throughout the organization relate to the cornerstones of corporate defense:

- Anticipation
- Prevention
- Detection
- Reaction

These four enterprise wide objectives should be present in the mindset throughout the organization. As individuals perform a variety of daily activities they should always be cognizant of these corporate defense drivers. Each staff member must fully understand the corporate defense cycle, be alert to the potential hazards and remain in a constant state of vigilance. The degree to which these unifying objectives are present in the corporate mindset throughout the organization could be said to represent the “DNA” of corporate defense, and will ultimately determine the organization’s success in dealing with the challenges it faces.

Conclusion

What the catalyst for corporate defense to play a more eminent role in corporate strategy will be remains to be seen. One thing however appears to be clear, defending the interests of the all stakeholders is a prerequisite for any future success, and Corporate Defense Management (CDM) is the best available option to achieve this objective.

Originally published by Source Media in DM Review (DM Direct) – December 2006

Author: Sean Lyons
Risk–Intelligence–Security–Control
R.I.S.C. International (Ireland)
sean.lyons@riscinternational.ie
www.riscinternational.ie