Corporate Intelligence and Its Role in a Corporate Defense Program

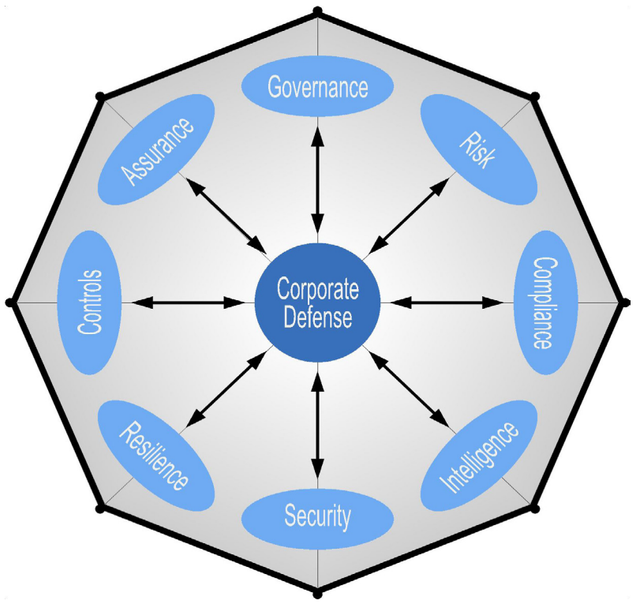
by Sean Lyons

Note: *This paper is based on the author's presentation at the SCIP European Summit in Cascais, Portugal on 15th November 2017*

Delivery of Sustainable Stakeholder Value in the 21st Century

A basic level of common sense would suggest that in the 21st century the delivery of sustainable stakeholder value requires an appropriate balance between the organization's focus on bringing the dollar in through the front door (value creation) and it's focus on preventing the dollar from leaving through the back door (value preservation). Intuitively, long term success in business requires a focus on both value creation (offense) and value preservation (defense). As the old sporting aphorism states, *offense wins games, but defense wins championships*. Long term success in business, as in sports, involves a prudent balance between offense and defense. Ongoing corporate failures suggest that getting the right balance between the focus on offense and the focus on defense can represent a considerable challenge for many organizations (Lyons 2014).

Figure 1. Corporate Defense Umbrella



In a business context, offense is typically associated with issues such as growing the business, profit generation, and a more immediate focus on short-term rewards, while defense is typically associated with issues such as the protection of assets, loss prevention, and a long-term focus on sustainability. Corporate health requires a healthy balance between these two complementary yet antagonistic principles, and it is important to appreciate that corporate health is similar to human health, as it improves when cared for and deteriorates when neglected. Unfortunately, in many organizations an imbalance often exists between the focus on offense and the focus on defense, and this imbalance results in what can be referred to as a defense deficit (Lyons 2012). Such a deficit reflects an organization's insufficient focus on its defense or value preservation obligations.

Defense Focus: The Corporate Defense Program

The term corporate defense is synonymous with value preservation as defense related activities are primarily concerned with defending against value erosion, reduction, or destruction. It represents the umbrella term used to describe an organization's collective program for self defense and the collective management of its defense related activities. At a cross-functional level every organization will have some form of corporate defense program in place whether this is by chance or by design. Unfortunately, however, such programs can often vary from documented formal structured programs in certain organizations to undocumented, implied unstructured programs in others. The degree of formality and structure present can in most cases represent a good indication of the organization's level of focus on defense.

In essence, a corporate defense program reflects the organization's ongoing efforts to manage a range of defense related disciplines which make up the corporate defense umbrella (Figure1). A comprehensive corporate defense program therefore requires a multi-disciplinary approach and involves aligning, coordinating, and integrating these eight distinct disciplines, each of which is considered to be a critical component of a robust corporate defense program (Lyons 2009a). These eight critical components are outlined as follows:

Critical Corporate Defense Components

- **Governance:** How the organization is directed and managed, all the way from the boardroom to the front-lines.
- **Risk:** How the organization identifies, measures, and manages the risks it is exposed to.
- **Compliance:** How the organization ensures that its activities conform with all relevant mandatory and voluntary requirements.
- **Intelligence:** How the organization ensures that it gets the right information, for the right purpose, in the right format, to the right person, in the right place, at the right time.
- **Security:** How the organization ensures that it protects its critical assets from threats and danger, its people, information, technology and facilities.
- **Resilience:** How the organization ensures that it has the capacity to withstand, rebound or recover from the direct and indirect consequences of a shock, disturbance or disruption.
- **Controls:** How the organization ensures that it has taken appropriate actions in order to address risk and to help ensure that the organization's objectives will be achieved
- **Assurance:** The system in place to provide a degree of confidence or level of comfort to the stakeholders that everything is operating in a satisfactory manner.

Each of these components needs to be incorporated into the organization's corporate defense framework in order to help ensure that they are managed in an appropriate manner. Organizations need to fully appreciate the positive contributions that each of these components provides, both individually and collectively. Effective corporate defense requires a clear understanding of the continuous interaction, interconnections, and critical interdependencies that exist between these components. It requires an understanding that the management of these complementary components continuously impacts the other in our increasingly complex corporate ecosystems. In fact, the symbiotic nature of their relationships means that each contributes to, and receives from, each of the other disciplines.

A collective approach to their management is required as recent developments in each of these disciplines has meant that the boundaries between these components have become somewhat blurred, and therefore, it is now increasingly difficult to determine where one component ends and another begins since each includes elements of the others. In essence, each of these components provides different but essential perspectives in dealing with potential hazards. For example, viewing any particular issue through a *risk-centric* lens will produce a different perspective than when viewing the same issue through a *compliance-centric* lens, etc. By incorporating these many different perspectives, an organization can help develop a more holistic view of any particular issue and be in a position to better avoid any potential cognitive bias or blind-spots that may otherwise exist (Skroupa 2016). The cross-referencing of each of these specialist disciplines can help provide the organization with a robust system of checks and balances and help to ensure that each of these disciplines becomes ingrained into day-to-day activities as well as the organization's DNA.

Ongoing Corporate Scandals

It is common for postmortem investigations into the causes of corporate scandals to typically identify deficiencies and weaknesses in the corporate defense program of the organization concerned. These deficiencies and weaknesses can begin with the non-existence of a formal corporate defense program, however, a selection of individual corporate defense matters are frequently identified. Typically examples of these issues can include the following:

- Failures in corporate governance
- Poor risk management

- Compliance failures
- Unreliable intelligence
- Inadequate security
- Insufficient resilience
- Ineffective controls
- Failures by assurance providers

The existence of more than one of these issues in any given organization tends to exacerbate any initial problems and can eventually result in exponential collateral damage to stakeholder value (Lyons 2016a).

Interestingly, in practically all cases, corporate scandals are deemed to be the result of poor decision making at some level within the organization. Typically poor decision making is associated with poor or inadequate intelligence, insufficient intelligence, unreliable intelligence, or some other form of intelligence failure. Make no mistake, intelligence professionals are never very far from scrutiny in such circumstances, and therefore, the important role of the intelligence component in a corporate defense program needs to be fully understood and appreciated.

The Intelligence Component

What exactly is meant by the intelligence component in this context? Intelligence, and the management of intelligence, is considered to be one of the critical components of an organization's corporate defense program. In simple terms, this refers to how the organization ensures that it gets the right information, for the right purpose, in the right format, to the right person, in the right place, at the right time (Lyons 2016b). Professor William E. Halal, Professor of Management at George Washington University, described an organization's intelligence component as follows:

"Organizational Intelligence (O.I.) is the capacity of an organization to create knowledge and use it to strategically adapt to its environment or marketplace. It is similar to I.Q. [Intelligence Quotient] but framed at an organizational level. While organizations in the past have been viewed as compilations of tasks, products, employees, profit centers and processes. Scholars have shown that organizations engage in learning processes using tacit forms of intuitive knowledge, hard data stored in computer networks and information gleaned from the environment, all of which are used to make sensible decisions. Because this complex process involves large numbers of people interacting with diverse information systems, O.I. is more than the aggregate intelligence of organizational members; it is the intelligence of the organization itself as a larger system" (Halal 1997).

Business by its very nature is complex, however, it is logical to say that the quality of an organization's intelligence will generally determine its long term success or failure. Intelligence is critically important because it helps an organization to understand complexities and helps inform decision making. Clearly successful organizations often display acute intelligence, the ability to learn quickly, and to successfully adapt to their ever-changing business environment. Less successful organizations often appear to display lower levels of intelligence, are much slower to learn, fail to detect signals of change, and hence, fail to respond accordingly. Therefore when considering intelligence as a distinct discipline within the corporate context, it is important to appreciate that the scope of the intelligence component is much more than traditional information reporting.

Intelligence is pervasive and it could, therefore, be said to encompass issues such as integrated thinking, knowledge management, information technology, and communications and organizational learning, etc. A prerequisite for success is ensuring and maintaining the breath, depth, and comprehensiveness of intelligence, enabling capabilities at all levels of the organizational structure. Intelligence enabling capabilities encompass mechanisms, processes, and systems. It also includes people as well as intelligence architecture and infrastructure (Bone 2017). In fact, the intelligence domain covers a very wide spectrum indeed. It can be viewed from numerous perspectives, from a very broad focus to a very narrow one. Such a wide and varied domain therefore presents its own unique set of challenges.

Examples of Intelligence-Related Activities		
- Strategic Intelligence	- Tactical Intelligence	- Operational Intelligence
- Competitive Intelligence	- Business Intelligence	- Market Intelligence
- Integrated Intelligence	- Organizational Learning	- Knowledge Management
- Information Management	- Information Technology	- Big Data
- Unified Communications	- Social Media	- Digital Transformation
- Management Reporting	- Financial Reporting	- Integrated Reporting
- Artificial Intelligence	- Cognitive Computing	- Machine Learning
- Content Management	- Record Management	- Archive Management
- Integrated Thinking	- Design Thinking	- Systems Thinking
- Intellectual Property	- Education and Training	- Complexity Science

The Intelligence Domain

Examples of a multitude of intelligence related activities, which could be classified as being within the intelligence domain, are outlined above and give an indication of the potential scope of the intelligence component.

Certain enlightened organizations may already be adopting a holistic view of corporate intelligence and be addressing most, if not all, of the above within a central corporate intelligence function under the responsibility of the Chief Intelligence Officer (CIO). In far too many organizations, however, many of these activities will be operating in isolation from one another within different functions such as the Information Technology (IT) function, the Operations function, or the Finance function, etc. This may also mean that responsibility for corporate intelligence related activities is spread out between many different roles, such as the Head of IT, the Head of Operations, or the Chief Financial Officer etc. Indeed in a growing number of organizations additional senior positions and roles such as the Chief Information Officer, the Chief Digital Officer, the Chief Technology Officer, the Chief Communications Officer, and the Chief Reporting Officer (to name but a few) are also now emerging (Biagini 2017). This list appears to be continually growing.

The Intelligence Program

Similar to a corporate defense program, every organization will have some form of intelligence program in place whether it is by chance or by design. And again, these can range from documented formal structured programs to undocumented implied unstructured programs. Unfortunately, in many organizations, there is a lack of a c*ollective intelligence* agenda (Mulgan 2017), and the management of many of these activities is somewhat dispersed and fragmented into different silos. In some cases they may be operating in a rather chaotic or disorganized manner as they often lack a sense of a unifying structure. Many of these activities have their own unique frameworks and specific representative bodies, which narrowly focus on the activity in question, in isolation of a broader collective intelligence agenda. Therefore unifying, aligning, and integrating all these intelligence-related activities under a single common vision within an organization remains a serious challenge. In fact, of all of the critical corporate defense components, the intelligence component is perhaps the most fragmented and was, at one point, the least mature, although it does appear that this is now beginning to change. As a result, it is increasingly being recognized that the intelligence component has the most to contribute, and potentially, has the brightest future.

Intelligence Deliverables

In many respects intelligence can be seen as representing the oxygen or lifeblood of an organization as it is linked to decision making at every aspect of the business, be it strategic, tactical, or operational. Therefore it is not very difficult to appreciate that the quality of the intelligence flow will have a direct impact on the quality of an organization's decision making and subsequent performance. As such the importance of the effective management of the intelligence component cannot be overstated, and should never be underestimated. The following are just some examples of what an effective intelligence system is expected to deliver.

- Accurate Intelligence
- Reliable Intelligence
- Relevant Intelligence
- Up-to-date Intelligence
- Objective Intelligence
- Accessible Intelligence

Most of these are self-explanatory and are certainly not new to intelligence professionals. To help achieve these objectives, intelligence controls will typically focus on integrity issues such as the validity, accuracy, and completeness of information, as well as issues such as confidentiality, availability, and timeliness of information. The precise nature of any given organization's specific intelligence requirements can vary depending on its industry, business type, and geographic location. Therefore each organization needs to establish its own precise intelligence requirements at strategic, tactical, and operational levels.

By integrating core intelligence principles into every aspect of decision making on an enterprise-wide basis, an organization can help ensure that it makes the best possible decisions, based on the best available intelligence. The generic intelligence objective outlined below should perhaps be the guiding light when addressing specific intelligence deliverables regardless of the issue in question.

Generic Intelligence Objective

Delivering [**What?**] the right information, [**Why?**] for the right purpose, [**How?**] in the right format, [**Who?**] to the right person, [**Where?**] in the right place, [**When?**] at the right time.

Intelligence and Corporate Defense

From the perspective of intelligence professionals, the intelligence component, in particular, plays an important part in the overall corporate defense program. For instance, the intelligence component is impacted by management as well as has impacts on the management of the other seven critical components. Therefore each of the other components should systematically address the intelligence element within their individual initiatives. This means that these initiatives need to consider intelligence requirements associated with their own area of expertise and address issues such as *governance intelligence, risk intelligence, compliance intelligence, security intelligence, resilience intelligence, controls intelligence,* and *assurance intelligence*. In each case, intelligence relates to the mechanisms, processes, and systems required to identify, obtain, interpret, and communicate the required data, information, and knowledge available both within and outside the organization itself. The goal in each case is to be in the best possible position to make the timely and informed decisions which are necessary for the achievement of each of the critical component's own objectives. Clearly intelligence is considered to be a critical component of a corporate defense program as all corporate defense related decisions are influenced by the available intelligence.

Conversely a comprehensive intelligence program should also systematically incorporate elements of the other critical corporate defense components. The intelligence component must give due consideration to the extent to which each of these elements is addressed within its own initiative. This means addressing issues such as *intelligence governance, intelligence risk, intelligence compliance, intelligence security, intelligence resilience, intelligence controls*, and *intelligence assurance*. Such a cross-functional approach requires inter-disciplinary co-operation, collaboration, and sharing of ideas.

The Intelligence Vertical

The provision of *defense-in-breath* and *defense-in-depth* requires a holistic view of corporate defense. In order to help the corporate defense program deliver these dual objectives the intelligence component must also view the organization's intelligence requirements from a holistic perspective. This means not only addressing its cross-functional (horizontal) intelligence requirements but also addressing its strategic, tactical and operational (vertical) intelligence requirements (Lyons 2016b). Due consideration should also be given to how the organization's intelligence requirements and responsibilities are being addressed throughout its various *lines of defense*.

A comprehensive lines of defense model includes the traditional three lines of defense, whereby operational line management is considered to be the first line of defense (LoD), tactical oversight functions (e.g. corporate defense functions) are considered to be the second line of defense, and independent internal assurance (e.g. audit committee and internal audit) is considered to be the third line of defense. Importantly, at a strategic level, it also includes executive management as the fourth line of defense and the board of directors as the fifth and final line of defense (Lyons 2011). This means addressing issues such as *board intelligence* (Libert et al 2017), *executive intelligence*, *3rd LoD intelligence*, *2nd LoD intelligence*, and *1st LoD intelligence*. The extent to which intelligence requirements and responsibilities are addressed at each of these lines of defense, both individually and collectively, will have a critical bearing on the success or failure of the corporate defense program.

Intelligence Alignment

Logically the intelligence component will add most value to the corporate defense program if its focus is in alignment with the defense focus. This also applies to its alignment with the corporate or business focus. In order to add value, a proactive intelligence program will need to be in alignment with both the corporate defense program and the overall business program. Ideally, these two will, themselves, already be in alignment, and if not, the organization may already have some rather serious issues to address.

It is, however, becoming increasingly evident that organizations seeking sustainable success need to ensure that they have a mature intelligence program in place. A mature intelligence program means that it has been integrated into these other programs at strategic, tactical, and operational levels. This means that the intelligence program needs be coordinated with these other programs so that they are all strategically aligned, tactically integrated, and operating in unison towards the achievement of common objectives.

It is becoming increasing obvious that intelligence professionals, in their own right, need to influence and be influenced by these broader programs. Ideally, they will become a necessary element of these broader programs. The degree to which an organization's intelligence professionals can influence these other programs is however very much up to the intelligence professionals themselves. The gradual elevation of corporate intelligence within the organization's hierarchy obviously presents numerous opportunities for those CIOs and other intelligence professionals who are prepared to stretch outside their comfort zones (Webb 2018).

For example, there is no practical reason why the CIO should not be setting the corporate defense agenda and actually become the driving force behind corporate defense over the coming years. There are an increasing number of opportunities presenting themselves to the CIO who appreciates the importance of connectional intelligence (Dhawan and Joni 2015) in this age of hyper connectivity. CIOs also need to be fully aware of the continuous developments in non-biological intelligence and the development of integrated technologies (Khan et al 2017). For this reason, the CIO is uniquely

positioned to be at the forefront of corporate defense leadership, however, the CIO is also likely to face stiff competition from, among others, the Chief Governance Officer, Chief Risk Officer, Chief Compliance Officer, Chief Security Officer, Chief Controls Officer, and the Chief Assurance Officer. Much may well depend on the current positioning of the CIO within the existing organizational hierarchy and the CIO's current status and sphere of influence.

Ten Intelligence and Corporate Defense Considerations

With this in mind, going forward intelligence professionals need to consider their organization's current approach to the intelligence component. Such consideration will help to establish its current focus on intelligence, its attitude towards intelligence, and its general prioritization of intelligence, not only within the corporate defense program but within the wider organization. The following issues should therefore be considered:

1. The seniority of the *intelligence champion* (the individual with overall responsibility for corporate intelligence within the organization) and the nature of their reporting line to the board of directors.

2. The extent to which the intelligence program happens to be in place, either by chance or by design.

3. The extent to which the scope of the intelligence program is viewed in broad holistic terms or in more narrow selective terms.

4. The extent to which the current intelligence program reflects a documented, formal structured program or an undocumented implied unstructured program.

5. The extent to which there is a formal intelligence charter in place and whether it has a formal intelligence vision, mission statement, and intelligence strategy in place.

6. The extent to which the organization has formalized its intelligence plan, its intelligence framework, and its intelligence policies, practices, and procedures.

7. The extent to which the intelligence strategy is in alignment with the overall corporate defense strategy.

8. The extent to which intelligence strategy is in cross-functional alignment with the other critical corporate defense component strategies so that they are all strategically aligned, tactically integrated, and operating in unison towards common objectives.

9. The extent to which the intelligence strategy focuses on the vertical intelligence requirements throughout all five lines of defense.

10. The extent to which the intelligence strategy is in alignment with the overall business strategy of the organization.

Reflection on the above considerations will help intelligence professionals to determine the current positioning of corporate intelligence within their organization and will also help to determine the opportunities and challenges awaiting these intelligence professionals going forward within their organization. Importantly, intelligence professionals need to always be cognizant that actionable intelligence leads to better decision making throughout the organization, and this needs to be convincingly communicated throughout the enterprise.

References

1. Biagini, Larry. (2017), Lessons from 2017: The Identity Crisis in the Technology C Suite, Forbes, 15th December, 2017, at www.forbes.com

2. Bone, James (2017), Intelligent Automation: Designing The Intelligent Organization, Corporate Compliance Insights, September 25, 2017, at www.corporatecomplianceinsights.com

3. Dhawan, Erica and Joni, Saj-nicole A. (2015), Get Big Things Done: The Power of Connectional Intelligence, Palgrave Macmillan, February 2015

4. Halal, William E. (1997), Organizational Intelligence: What Is It, and How Can Managers Use It?, Strategy + Business, October 1997

5. Khan Naufal, Lunawat Gautam, Rahul Amit, (2017), Toward an integrated technology operating model, McKinsey & Co., October 2017, at www.mckinsey.com

6. Libert, Barry, Beck Megan, Bonchek Mark, (2017), AI in the Boardroom: The Next Realm of Corporate Governance, Sloan Management Review, October 19, 2017, at www.sloanreview.mit.edu

7. Lyons, Sean (2009a), Corporate Defense Insights: Dispatches from the Front Line, Continuity Central, March 2009, at www.continuitycentral.com

8. Lyons, Sean (2011), Corporate Oversight and Stakeholder Lines of Defense, The Conference Board Executive Action Report, No. 365, October 2011

9. Lyons, Sean (2012), Achieving a Healthy Balance Between Offense and Defense in 21st Century Capitalism, HBR/McKinsey M-Prize for Management Innovation – The Long Term Capitalism Challenge, Management Innovation Exchange, 26th April 2012, at www.managementexchange.com

10. Lyons, Sean (2014), Striking A Balance: Offence v Defence, Ethical Boardroom Magazine, Winter 2014

11. Lyons, Sean (2016a), Bulletproof your defence: The role of the board in delivering a robust corporate defence programme, Ethical Boardroom Magazine, Spring 2016

12. Lyons, Sean (2016b), Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program, CRC Press, September 2016

13. Mulgan, Geoff (2017), Big Mind: How Collective Intelligence Can Change Our World, Princeton University Press, October 2017

14. Skroupa, Christopher (2016), Evaluating Corporate Defense Through Different Lenses, Forbes, July 2016, at www.forbes.com

15. Webb, Geoff (2018), The Evolving Role Of The CIO In 2018, Forbes, 9th January 2018, at www.forbes.com

ABOUT THE AUTHOR

Sean Lyons *is an internationally recognized corporate defense author, pioneer, and thought leader. Sean is published internationally and has lectured and spoken as a keynote speaker and a subject matter expert at lectures, seminars, and conferences in Europe, North America, and Asia. As the architect of the cross-functional discipline of Corporate Defense Management (CDM), he is widely regarded as the foremost authority in this emerging field. Sean is the author of the critically acclaimed book entitled,* ***Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program.***