EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

JULY 2009 VOL. XL, NO. 1

OPTIMIZED CORPORATE DEFENSE PROGRAMS: A 5 STEP ROADMAP

SEAN LYONS

The corporate world finds itself staring into an economic abyss that some believe was of its own making. On reading a recent *Harvard Business Review* article entitled "How to Thrive in Turbulent Markets" (Sull, 2009), I began wondering just how much the corporate world could potentially learn from the world of sport. The article suggested that true champions, be they in the boxing ring or the corporate arena, require both agility and absorption (qualities normally associated with defensive skills) in order to prevail. It occurred to me that perhaps it is the different value placed upon defensive skills that most clearly sets these two worlds apart.

DEFENSIVE SKILLS: A SPORTING PERSPECTIVE

In team sports in particular there is a real appreciation of the requirement to focus on both offensive and defensive strategies and tactics in order to ensure that these are successfully implemented in the field of play. There is a clear understanding of the relationships that exist between the interaction of both offensive and defensive personnel and how collectively as a team there is a requirement to have an appropriate balance between these two inter-dependent disciplines. Coaches are aware that in order to be successful on the field of play, the team as a whole needs to be able to both attack and defend as required, and be capable of turning defense into offense and vice versa as the occasion demands. Many teams have specialist coaches for both their offensive and defensive units and these coaches are dedicated to helping to develop the diverse skills required in order to execute their strategies and tactics effectively.

If we are to focus on the defensive unit we see that defensive coaches are very much aware that the defensive unit as a whole is made up of individual specialist positions that need to be filled by players of suitable character and ability. Developing the unit begins with recruiting the required squad of individuals and by coaching these individuals on the necessary technical skills required. The selection of the starting line-up is based on the players best suited to

Taylor & Francis
Taylor & Francis Group

address the team's defensive requirements. These selected players must then be coached on how to play as a cohesive defensive unit. This unit must then learn to play and interact with the offensive unit as a team so that all the players involved are contributing to the greater common goal. Finally the team must learn to continually develop both its individual and collective skills in order to constantly improve, and in order to reach the increasingly higher levels of performance required if they have any ambitions of achieving success.

The head coach is aware of the necessity for the offensive and defensive units to be able to operate in unison and therefore his or her job is to ensure that both of these two units interact as cohesively as possible. He or she recognizes that any success will depend on blending these two antagonistic yet complementary disciplines, as winning in team sports generally involves outscoring the opposition and this requires the performance of both these disciplines. Successful teams tend to be built on the foundations of a solid defensive unit; moreover, the higher up the field the defensive tactics come into play the more protection is offered to its vulnerable areas. Winning trophies involves a balanced investment in both those whose role it is to take scores, and those whose role it is to prevent conceding scores. The secret to sporting success is to get the right balance between the two.

DEFENSIVE SKILLS: A CORPORATE PERSPECTIVE

Unfortunately, defensive skills in the corporate context are rarely held in such high regard and a glaring imbalance exists in relation to the appreciation of the critical requirement for both offensive and defensive activities. In the corporate world rarely (if ever) are those with responsibility for preventing the dollar from going out the back door held in the same high esteem as those with responsibility for bringing the dollar in the front door. Defensive activities have traditionally been mocked as "business prevention centers" (Masters & Tucker, 2009), often considered as no more than pure cost centers that stood in the way of making money. As we have seen in recent times the result of such an attitude can be catastrophic, the financial tsunami being an obvious example.

Interestingly, although the term "corporate defense" has been in use for many years and is perhaps intuitively understood, its

If you have information of interest to *EDPACS*, contact Dan Swanson (dswanson_2008@yahoo.ca). *EDPACS* (Print ISSN 0736-6981/Online ISSN 1936-1009) is published monthly by Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106. Periodicals postage is paid at Philadelphia, PA and additional mailing offices. Subscription rates: US$ 300/£181/€240. Printed in USA. POSTMASTER: Send address change to *EDPACS*, Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106.

specific meaning can differ from person to person and indeed from organization to organization. Its precise definition can also vary depending on the circumstances in which it is applied. Typically it is addressed only as a reactive response to pending litigation or is only seen in a very narrow focus such as security or compliance issues. As a result the very objective of defending the organization appears not to be fully understood or indeed its requirement not fully appreciated. While many defense-related activities are employed by organizations to help to safeguard and mitigate against risks, threats, and hazards, all too commonly these activities are very often not managed in a coordinated manner and are therefore not operating in unison toward common goals and objectives. Frequently they actually operate independently and in isolation of one another in silo-type structures. Ironically, however, these activities do share a common high-level objective, that of helping to defend the organization, and therefore it could be said that they represent different lines of defense, or multiple layers of defense. Corporate defense therefore in its broadest sense could be said to represent an organization's collective program for self-defense.

THE CRITICAL COMPONENTS OF A PROGRAM FOR SELF-DEFENSE

Any comprehensive program for self-defense requires a number of related components to be operating in unison in order to be successful. Eight core defensive activities that need to be managed have been identified and are deemed to represent the critical components that constitute an organization's program for self-defense (Lyons, 2009).

- Governance
- Risk
- Compliance
- Intelligence
- Security
- Resilience
- Controls
- Assurance

As in the sporting context the entire defensive unit needs to be managed in a coordinated and cohesive manner before it can successfully interact with the other business activities.

Governance

Management of the governance component is required in order to help ensure there is a system in place to address how the organization is directed and controlled, all the way from the boardroom to the factory floor. It involves specifying the distribution of rights and responsibilities among different stakeholders and spelling out the rules and procedures for decision making. It therefore involves multidimensional layers, both vertical and horizontal, which reflect the measures and mechanisms in place throughout the organization for setting and achieving organization objectives and the

means for monitoring performance. The governance component therefore not only impacts all of the other defensive components at strategic, tactical and operational levels but also its impact is felt throughout the entire enterprise.

Risk

Management of the risk component is required in order to systemically address how the organization identifies, measures, and manages the risks it is exposed to, whereby risk is understood as the uncertainty or possibility that an event will occur that can have an adverse impact on the achievement of the organization's objectives. Risk management is therefore concerned with addressing the relationship between potential risks and their related potential rewards while ensuring that risk exposures are in line with the organization's risk appetite. While inherent risk can perhaps be established in isolation, an organization's residual risk can only be satisfactorily determined after considering the organization's capabilities in relation to the other critical components.

Compliance

Management of the compliance component is required in order to help ensure the organization's activities are in conformance with all relevant mandatory and voluntary requirements. It involves clearly defining applicable laws, regulations, codes, best practices and internal standards, and so on, and how the organization can demonstrate how it manages to ensure that it is in strict adherence with all relevant requirements. The management of the compliance component is both impacted by, or impacts, all of the other critical components.

Intelligence

Management of the intelligence component is required in order to help ensure that the organization gets the right information, to the right person, in the right place, at the right time. It relates to mechanisms, processes, and systems in operation as an organization identifies, gathers, interprets, and communicates the information and knowledge available within (and outside) the organization in order to be in the best possible position to make the timely and informed decisions that are necessary for the achievement of its objectives. It refers to both the larger organization's capacity to create and use intelligence and the aggregate intelligence capacity of its stakeholders. The intelligence component is therefore a critical element in the management of all the other critical components.

Security

Management of the security component is required in order to help ensure that the organization has the ability to protect their assets (i.e., people, information, technology, and facilities) from threats or danger. This involves the ongoing management of both physical and logical security issues in order to secure the assets of

the organization. It requires the deterrence, prevention, or preemption of threats facing the organization and mitigating these threats or minimizing any possible vulnerability that might exist. Assessing security requirements and planning for appropriate levels of asset protection involves consideration of each of the other critical components. Management of the security component is both impacted by, or impacts, all of the other critical components.

Resilience

Management of the resilience component is required in order to help ensure that the organization has the ability to withstand, rebound, or recover from the direct and indirect consequences of a shock, disturbance, or disruption. It is about focusing on its ability to sustain the impact of an emergency or interruption, and its capacity to recover from a disaster scenario, in order to resume its operations and continue to provide services with a minimum impact on performance and productivity. Organizational resilience relates to sustainability and involves adapting to the constantly changing business environment. It represents an organization's ability to keep its business critical processes, services, and assets up and running in the face of adversity. The resilience component is also both impacted by, or impacts, the management of all of the other critical components.

Controls

Management of the controls component is required in order to help ensure that appropriate actions are taken by the organization in order to address risk and in the process help ensure that the organization's objectives and goals will be achieved. These actions include the practices and procedures employed by the organization in order to provide the board with at least reasonable comfort that the organization's objectives will be achieved in an effective, efficient, and economical manner. The controls themselves may be either preventative or detective and can be either manual or automated. The terms *control culture* or *control environment* refer to the continuous operation of controls at all levels within the organization. The control component therefore has a significant impact on the management of each of the other critical components.

Assurance

Management of the assurance component is required in order to help provide a degree of confidence or level of comfort to the stakeholders of the organization. It involves the independent expression of a conclusion about the assessment or evaluation of the particular subject matter against specific pre-defined criteria. This requires the performance of an objective examination of evidence, in order to provide an impartial assessment on a particular subject matter. The assurance component includes an evaluation of both the management and the operational performance of all of the other critical components.

CORPORATE DEFENSE–RELATED ACTIVITIES

Corporate defense is therefore about acknowledging that each of the aforementioned components are inherently interdependent, interlinked, and interconnected, and as such all can impact on one another, leading to what has been referred to as a symbiotic-type relationship. It also has to be appreciated that these core components cover a multitude of defense-related activities, all of which can require specialist skills, knowledge, and experience. Corporate defense is about understanding that each individual component requires varying levels of expertise and it is therefore unreasonable to expect any one person in an organization to be considered an expert in all these areas. Examples of the issues addressed by these components include those listed in Table 1.

Functional Developments in This Area

In recent years in particular there has been significant developments in each of these defense-related activities, so much so that it

Table 1 ***Examples of Corporate Defense Activities***

Governance

- Culture/Environment/Ethics
- Stakeholder Relations
- Design/Structure
- Strategy/Planning
- Corporate Responsibility
- Accountability
- Framework
- Methodology

Risk Management

- Enterprise Risk
- Business Risk
- Strategic Risk
- Operational Risk
- Credit Risk (excluded)
- Market Risk (excluded)

Controls

- Internal Controls
- Financial Controls
- Operational/Processing Controls
- Supervisory Controls
- Compliance Controls
- Security Controls
- Preventative/Detective Controls
- Primary/Compensating Controls

Assurance

- Inspection Review
- Internal/External Audit
- Regulator Review
- Rating Agency Review
- Standards Certification
- Self Assessment Review
- Due Diligence Review
- Fraud Examination
- Forensic Investigation
- Litigation Support
- Asset Recovery

Resilience

- Emergency Operations
- Crisis Management
- Disaster Recovery
- Contingency Planning
- Continuity Management
- Incident Response Management
- Health & Safety
- Insurance

Compliance

- Regulatory Compliance
- Legal Compliance
- Workplace Compliance
- Industry Codes
- Best Practice Guidelines
- Internal Standards

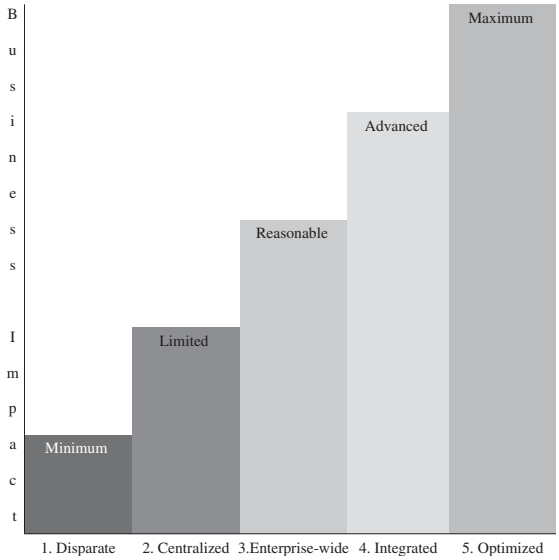
Intelligence

- Business Intelligence (B.I.)
  - Operational Intelligence
  - Market/Competitive Intelligence
- Knowledge Management
  - Content Management
  - Record Management
  - Document Management
  - Filing/Storage/Archiving Management
- Communication

Security

- Physical Security
  - Premises Security
  - People Security
  - Information Security
  - Facility Security
  - Operations Security
- Logical (I.T.) Security
  - Client Security
  - Application Security
  - Operating System Security
  - Database Security
  - Network Security
  - Gateway Security

Figure 1 ***Functional maturity model.***



has been referred as an evolutionary process that is commonly described in terms of a maturity model (Figure 1). This evolution seems to be occurring in practically all of these components, although some are generally at a more advanced phase of maturity than others. The maturity models applied, of which there are many variations, are generally based on an adaptation of the capability maturity model (CMM), which was developed for defense software purposes by the Software Engineering Institute (SEI) at the Carnegie Mellon University in the mid-1980s (Humphrey, 1989). Derivatives of this maturity model can be found in practically all of the defense-related activities referred to earlier.

Phases of Development

The Disparate Phase

Initially the individual business units within the organization tend to be left to their own devices in developing their approach or methods in relation to the management of any one of these components, representing something of a disparate or fragmented-type approach. This often results in these approaches being developed on an inconsistent basis and consequently the management of a given component across the business units is generally unsystematic and unstructured (e.g., ad-hoc risk management). The business impact associated with this phase of development is considered minimum as the activity tends to be performed in an ad-hoc manner and often operates in a crisis management mode whereby the business unit is continuously fire-fighting on a day-to-day basis.

The Centralized Phase

In order to help develop a more consistent approach organizations next attempt to consolidate a particular component by introducing a centralized function. These centralized functions have responsibility for managing the component from a centralized source requiring specialist skills and expertise (e.g., risk management function). This phase could be described as 1st generation convergence, pulling related issues together under one umbrella, using a centralized-type approach. The business impact associated with this phase of development is improving but is still considered to be limited. The activity is now seen as a specialist area and is considered a defined professional discipline within the organization.

The Enterprise-Wide Phase

The next phase of maturity is designed to involve a push to embed agreed specialist principles and processes associated with the component throughout the entire organization or on an enterprise-wide basis. This promotion of an enterprise approach is an attempt to help ensure that all areas within the organization are adopting common practices so that all areas are addressing the relevant component in a systematic and structured manner (e.g., ERM program). The business impact associated with this phase of development is now considered to be increasing to reasonable as the organization now agrees on its enterprise objectives and to a defined set of methodologies that are required to be the standard or benchmark for a particular component's activity.

The Integrated Phase

The next phase of maturity involves an organization's attempt to integrate the component's activities by taking advantage of advances in technology. Such an integrated approach is the natural progression beyond the enterprise-wide phase to where a component's activities are now integrated, enabling the organization to effectively manage the activity by migrating from a manual to an automated environment (e.g., integrated risk solution). By using available technological solutions it is now becoming possible for organizations to move toward an end-to-end vertical and horizontal integration of the component's activities. The business impact associated with this phase of development is now considered advanced as it becomes possible to report essential measurement metrics relating to performance and productivity.

The Optimized Phase

The final maturity phase involves the organization focusing on deliberate process improvement and optimizing the use of the organization's resources. This is possible because the organization now has it people, processes, and systems fully integrated, and its workforce has now become empowered. The business impact associated with this phase of development represents the organization's opportunity to deliver maximum impact. By constant efforts at continuous improvement and by adopting accelerated learning techniques, the organization helps ensure that processes are continually enhanced and that performance becomes more innovative.

This phase involves continually improving process performance through both established and pioneering improvements. Quantitative and qualitative improvement objectives are determined, continually revised to reflect changing business objectives, and used as benchmark criteria in managing improvement. Both the defined goals and the organization's set of benchmarks are targets for constant evaluation and assessment (e.g., optimized risk management).

Cross-Functional Developments

Given that the aforementioned developments are occurring across various existing functions this can give rise to certain cross-functional operational inefficiencies. In an attempt to address some of the cross-functional issues that arise, similar developments are now also occurring at a cross-functional level. What is now emerging is an evolution in cross-functional convergence, in what could be referred to as 2nd generation convergence in this space. These cross-functional developments represent a reaction to the functional silo-type environments that have developed over time within organizations, and represent an attempt to reduce the resulting operational inefficiencies.

If we look at security management, at a functional level there is now a move toward 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 one that 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 life blood of any organization. We are now hearing terms such as "Enterprise Business Intelligence" (Eckerson & Howson, 2005) and indeed "Risk Intelligence" (Apgar, 2006) more and more. In North America in particular there is now a move beyond enterprise risk management (ERM) toward 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). Lately the term "Integrated Assurance Framework" has emerged in the controls and assurance environment. An integrated assurance framework is fundamentally concerned with the practicalities of bringing together risk, compliance, governance and audit. This framework represents an attempt to reengineer the assurance operating model so that values and synergies can be unlocked. By linking these areas it is hoped that organizations can create a more dynamic and sustainable assurance model. On the resilience side, perhaps concepts such as organizational, operational, and business resilience go even further, as resilience is now viewed not only as business continuity and disaster recovery (BCDR) but increasingly in terms of a number of other imperatives, which also encompass compliance and risk management as well as security and intelligence perspectives (IBM, 2004). The

emerging cross-functional discipline of corporate defense management (CDM) (Lyons, 2006) is an attempt to go beyond all of these developments and actually integrate and align the management of all eight of the critical components within the one program. Thankfully, what is now occurring is a re-thinking of the restrictive traditional mindset that was perhaps previously our biggest stumbling block (Knowledge@Wharton, 2009). Future progress will hopefully be spurred on by the lessons we are now learning as a result of the current financial crisis (OECD, 2009); specifically, in relation to weaknesses in our traditional safeguard systems.

CROSS-FUNCTIONAL MATURITY MODEL: A 5 STEP ROADMAP

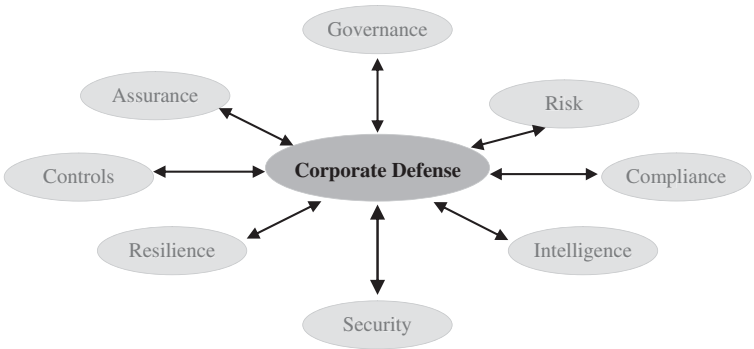
The concept of introducing a corporate defense program that integrates all of these critical components has a definite commonsense appeal and the presence of a director of Corporate Defense at the board level would supply the much-needed board counterbalance (Figure 2).

Many commentators have, however, expressed reservations as to the complexity of implementing such a program. The solution to this perceived dilemma is, however, perhaps more simple than many realize. Rather than introducing yet another new framework, organizations need to carefully re-organize their existing activities into a more efficient structure and actually leverage from the work already being done. Simply by taking a more strategic cross-functional view, organizations can quite easily apply the functional maturity model referred to earlier, only this time apply it in a cross-functional context. The resulting cross-functional 5 step roadmap is briefly outlined as follows.

Step 1: The Disparate Phase

Step 1 is to recognize the organization is currently operating in the disparate phase. At a cross-functional level this phase represents an organization with a traditional view of corporate defense as its defense components tend to operate in silo-type structures. This

Figure 2 ***Critical components of a corporate defense program.***



means that they are not in alignment with one another, but rather they operate in isolation as 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 as each activity is operating toward its own narrow view and objective, and as a result they can very often be the subject of internal power struggles. Very often the overall responsibility and accountability for corporate defense is dispersed or fragmented, diluted or ambiguous. In certain scenarios it can sometimes even be non-existent.

The cross-functional organizational value associated with this phase of development is considered minimum. In fact, as a consequence of this type of traditional mindset, an organization can be subject to typically negative impacts. Confusion relating to overall responsibility and accountability can result in omissions or gaps, and these in turn can create vulnerabilities that can later be exploited, rendering many other related best efforts ineffective in the process. Silo-type structures typically result in multiple intersections, duplications, and overlaps of activities that can result in considerable inefficiencies and unnecessary redundancies from an operational perspective. In worst- case scenarios the power struggles that can occur from silo-type environments can actually develop into full-scale turf wars, and this can be extremely detrimental to its corporate health and leads to the creation of a dysfunctional organization.

Step 2: The Centralized Phase

Step 2 is to move toward consolidating all of these critical components under one umbrella and introduce a centralized unit or function. At a cross-functional level this phase represents an organization that is developing a strategic view of corporate defense and a more comprehensive understanding of the complexities of the task of managing the critical components collectively. There is now recognition of both the links and interconnections that exist between the organization's defense-related activities and the symbiotic nature of their interdependence. There is also a clearer appreciation of the correlations that exist between these activities and the possible cascade of consequences that can result, not only direct 1st order consequences but indirect 2nd and 3rd order consequences that can occur further down the road.

The cross-functional organizational value associated with this stage of development is improving but is still considered to be limited. By converging all of these components under a unified management approach the organization can help to eliminate any confusion that may exist in relation to responsibility and accountability, which in turn diminishes the potential negative issues that can result from any lack of clarity. Corporate defense is now recognized as a holistic discipline requiring a strategic focus and begins to acquire appropriate status and authority within the organization. There is also the opportunity to introduce an improved stakeholder focus in terms of the strategically safeguarding the varying interests of its multiple stakeholders.

Step 3: The Enterprise-Wide Phase

Step 3 is to take the organization to the next level by focusing on ensuring that the organization's corporate defense philosophy and standards are tactically embedded into the culture of the enterprise. From a cross-functional perspective this phase represents a move toward a more sustainable approach to defending the organization as it now knows exactly where it needs to go, knows how to get there, and recognizes the need to build the required components into their tactical processes. Agreed standards form the basis for the consistent application of corporate defense throughout the organization. The resulting tactical planning will help align defense policies and best practices and will also help in the education of the organization.

The cross-functional organizational value associated with this stage of development is now considered to be increasing to reasonable as enterprise standards are now in place, enabling the adoption of a coherent approach to corporate defense throughout the organization. As consistent policies are applied there are now similar expectations in all areas, as the organization is now able to manage its corporate defense in a systematic manner, which means that where intersections do occur they can now be engineered in a structured manner. The result is cost savings associated with the identification and elimination of duplications, and reductions in overlaps and redundancies that were inherited from the silo-type environment.

Step 4: The Integrated Phase

Step 4 represents a move toward a seamless real-time integration of its corporate defense components. From a cross-functional perspective this phase represents both the vertical and horizontal integration of its people, processes, and systems via a cybernetic loop that enables the real-time communication of intelligence that is vital in order to make accurate and timely decisions. This level of integration facilitates the achievement of both top-down and bottom-up buy-in among management and staff, which is necessary to encourage increased operational collaboration and knowledge sharing across all of the components. It also helps to foster cross-functional support, which is required to ensure corporate defense becomes part of the organization's DNA at a procedural level. Responding to the business needs of more progressive organizations, many leading vendors in this space are now developing and providing end-to-end technology solutions that are enabling this level of integration to become possible.

At this phase of development an organization now begins to see superior value being added in this space. The organization now has fully integrated reporting in place for its corporate defense activities and has now determined its essential measurement metrics. This means that goals now become quantifiable and therefore performance becomes more predictable. Using these measurement metrics, management can now begin to anticipate and evaluate its corporate defense performance in totality. Management can now determine methods to modify and amend its corporate defense procedures to suit particular circumstances without significant

reductions in quality or divergence from its defined benchmarks. Its defense activities are now operating in unison toward common objectives resulting in increased transparency and accountability. There is now improved process alignment, resulting in further reductions in associated costs, thus leading to superior efficiency and effectiveness while at the same time also resulting in enhanced stakeholder support.

Step 5: The Optimized Phase

Step 5 represents arriving at the phase whereby the organization is now optimizing the use of its corporate defense resources. By further education and partnership the organization begins to empower its workforce, thus enabling it to unlock its latent potential. Through this partnership the organization now has the opportunity to further synchronize and synthesize its cross-functional activities, creating an optimization of its capabilities. This involves leveraging operational processes and maximizing the possible synergies that exist. Optimized processes are flexible, adaptable, and innovative, dependent on the participation of an empowered workforce, and the alignment with business values and the objectives of the organization. By focusing on the pursuit of excellence, practices begin to evolve in a flexible and adaptable way. Through constant vigilance the organization is now able to accelerate its reaction times in terms of anticipating, preventing, detecting, and reacting to potential vulnerabilities, thereby improving its preemptive capabilities and reducing potential liability. By collectively defending the organization the robustness of its defense program is hardened, resulting in both increased resilience and ultimately increased stakeholder comfort.

At this phase of development an organization now begins to realize optimal value from its defensive investments. Constant revision results in process streamlining leading to optimal efficiency and effectiveness and resulting in sustainable value creation. The effects of the organization's efforts to improve activities are now assessed and evaluated against the quantitative and qualitative improvement benchmarks. The organization's ability to rapidly react to changes and identify opportunities is enhanced by finding ways to accelerate learning and share knowledge. At this phase, business processes are concerned with addressing root causes of process exceptions, variations, and anomalies, and continuously adapting its processes in order to constantly improve business performance and productivity. This means diminishing overheads, improved performance, and increased productivity resulting in a competitive advantage for the organization.

CONCLUSION: THE BUSINESS CASE

It becomes apparent from the aforementioned roadmap that organizations only really begin to derive a positive return on their often significant investment in defense-related activities once they begin to arrive at step 3, the enterprise phase, and beyond. Ultimately, in an increasingly competitive environment this is where successful organizations need to be. In a time of economic downturn organizations

need to be optimizing value while minimizing overhead and redundancy.

The imperative for an organization to implement a comprehensive and holistic corporate defense program becomes more obvious when one focuses on the potential benefits of such an approach. Such a program facilitates the alignment of defensive objectives with the business objectives of the organization in order to help ensure that both the defensive and offensive units are operating in unison toward a common vision. A holistic approach to corporate defense can help provide additional comfort to stakeholders and help restore confidence in the organization where there once was doubt. It represents a tangible indication of the adoption of a more proactive approach to defending stakeholder interests and such an increased stakeholder focus can result in improved stakeholder retention. By unifying the management of defense-related activities an organization creates a more robust defensive unit and begins to foster a culture of collective responsibility, which is necessary to keep pace with growth, while at the same time meeting required standards. By accelerating the organization's reaction times to potential hazards the organization strengthens its preemptive capabilities, thereby reducing potential vulnerability. This helps to further protect profitability by eliminating potential liability in the process. Organizational resilience is maintained by continuous improvement and constant learning, which can result in strategic advantage through unlocking the latent potential of the organization and enabling a genuine pursuit of excellence in execution. This means leveraging synergies and optimizing resources through partnership and integration, thus allowing for increased operational efficiencies and improvements in performance and productivity.

It seems the sporting world has been much quicker than the corporate world to recognize that sustainable success can only be obtained through a blending of the skill and ability of its defensive and offensive activities. The adoption of the practical measures outlines in this article will help address many of the corporate governance shortcomings already identified and help ensure that the mistakes of the past will not be repeated again in the future. I for one look forward to the day when the defense element in the corporate equation is no longer seen in a negative light but becomes the normal expectation of its stakeholders in terms of both a business requirement and corporate social responsibility.

References

Apgar, D. (2006). *Risk Intelligence: Learning to Manage What We Don't Know*. Boston, MA: HBS Press.

Eckerson, W., & Howson, C. (2005, August). Enterprise business intelligence: Strategies and technologies for deploying BI on an enterprise scale. The Date Warehousing Institute (TDWI). Retrieved October 4 2006 from TDWI Website: http://www.tdwi.org/research/display.aspx?ID=7744.

Humphrey, W. (1989). *Managing the Software Process*. Reading, MA: Addison Wesley.

IBM (2004). Business resilience: Proactive measures for forward looking enterprises. Retrieved November 1 2006 from IBM Website: http://www-935.ibm.com/services/us/bcrs/pdf/br_business-resilience.pdf.

Knowledge@Wharton (2009, April 15). Re-thinking risk management: Why the mindset matters more than the model Retrieved from University of Pennsylvania Website: http://knowledge.wharton.upenn.edu/articlepdf2205.pdf?CFID=9537841&CFTOKEN=17956399&;sessionid=a830611373f6a8cf059554b777de525a4.

Lyons, S. (2006, November 15). An executive guide to corporate defence management (CDM). The RiskCenter. Copies available from the author at sean.lyons@riscinternational.ie.

Lyons, S. (2009, April 6). Corporate defense insights: Dispatches from the front line. The RiskCenter. Copies are available publicly at Social Science Research Network (SSRN), http://papers.ssrn.com/sol/3/papers.cfm?abstract_id=1337635.

Masters, B. & Tucker, S. (2009, April 21). Banks invest in compliance and risk monitors. *The Financial Times*. Retrieved from *The Financial Times* Website: http://www.ft.com/cms/s/79e9f1c8-2dd4-11de-9eba-00144feabdc0,Authorised=false.html?_i_location=http://www.ft.com/cms/s/0/79e9f1c8-2dd4-11de-9eba-00144feabdc0.html?ftcamp=rss&_i_referer=&ftcamp=rss.

Sull, D. (2009, February). How to thrive in turbulent markets. *The Harvard Business Review*. Retrieved from http://hbr.harvardbusiness.org/2009/02/how-to-thrive-in-turbulent-markets/ar/1.

The Alliance of Enterprise Security Risk Management (AESRM). (2006). Retrieved August 15 2007 from AESRM Website: http://www.aesrm.org.

The Open Compliance and Ethics Group (OCEG). (2007). The GRC illustrated series. Retrieved November 20 2006 from OCEG Website: http://www.oceg.org.

The Organisation for Economic Co-operation and Development (OECD). (2009, February 23). The corporate governance lessons learned from the financial crisis. Retrieved May 16 2009 from OCEG Website: http://www.oecd.org/dataoecd/32/1/42229620.pdf.

Sean Lyons, Principal, R.I.S.C. International (Ireland). Sean Lyons has amassed over two decades of experience working as an Internal Auditor, Operational Troubleshooter and Management Consultant. As a writer and speaker he is considered an active pioneer within in the contemporary corporate defense movement, being a firm advocate of the requirement for corporate defense to play a more eminent role in corporate strategy. Sean's vision is that each organization's corporate defense program will address the management of all aspects of governance, risk, compliance, intelligence, security, resilience, controls and assurance, in a coordinated and integrated manner. Selected publications are available at http://ssrn.com/author=904765.