ICPAK Forensic Audit Conference 2016

Theme:

Emerging fraud trends in the current corporate world

Topic:

Corporate Security, Governance and Risk Assessment

Date:

11th August 2016

Author:

Samuel N Kibaara; FIRM, ACBCI
Enterprise Risk and Business Continuity professional
Contacts: Email – skibaara@yahoo.com
Cellphone: +254 722 606 497

INTRODUCTION

Doing business is getting more and more complex. The over-whelming force of globalization has changed the structure and pace of corporate life. At the same time, security risks have become more complex, too. Many of the threats, such as terrorism, organized crime and information security, are asymmetric and networked, making them more difficult to manage. There is also greater appreciation of the interdependence between a company's risk portfolios

Corporate security is a term used to refer to the practice of protecting a business' employees, physical property and information systems. Corporate security identifies and effectively mitigates or manages, at an early stage, any developments that may threaten the resilience and continued survival of a corporation. Organisations are rapidly adapting to the changed environment from operational security management to strategic security management. Core elements of Corporate Security are:

1. Personal security
2. Physical security
3. Information security
4. Corporate governance
5. Compliance and ethics programs
6. Crime prevention and detection
7. Fraud deterrence
8. Investigations
9. Risk management
10. Business continuity planning
11. Crisis management
12. Environment, safety and health

From the above list it is now clear that corporate security sections have increasingly taken a central role in the operation of any organisations. Corporate security departments now have responsibilities in areas such as corporate governance, information assurance, business continuity, reputation management and crisis management, which is causing many to question the relevance of the term 'security' to describe what they do. The term resilience now more accurately reflects the range of their responsibilities

DNA OF SUCCESSFUL CORPORATE SECURITY IN TODAY'S GLOBAL WORLD.

There are a number of global companies/organisations that are successful in corporate security management. These companies have stood out is NOTbecause of state-of-the-artsecurity technologies, world-beating anti-fraud procedures orsecurity departments full of security experts, although some maywell have these attributes. Instead,these companies understand thatthe challenge for corporate security is no different from that for anyother function – they must keep pace with their company'schanging business environment and ensure that how they work,what they do and how they behave reflect these realities. They donot take their lead from terrorists, criminals and hackers – theybelieve that business imperatives drive security, not the other wayaround. These departments see their role as being changemanagement rather than

enforcement and focus on integrating asecurity dimension into the way the company does business.

MANAGING SECURITY WITHIN A CORPORATE GOVERNANCE FRAMEWORK

One of the most important business drivers impacting on security is corporate governance. As companies become increasingly aware of the interdependencebetween security risks and operating practices, security and corporategovernance have converged.Security has taken a much bigger role in this, and responsibility for it is now shared with the head of group audit and thecompany secretary. Many organisations reckon that managing security within agovernance framework has been helpful in achieving compliancefrom colleagues and visibility across the company. The problemat that stage is to get people to comply with them. The policies are now more visible at senior levels thanthey were previously. There is a greater level of assurance than there wasdoing before. This is having an impact on the shape and role of the corporatesecurity department.
First, it now has a much wider range ofresponsibilities. Recent thinking in the global security arena argues thatcorporate governance is one of five key factors meaning that thecorporate security department is now responsible for a wider range ofrisks, including *fraud*, *corruption*, *negligence*, *information securityand assurance*, *money laundering, business continuity planning,regulation*, *employee conduct*, and *the response to major eventsincluding natural and man-made disasters*.

The Challenges of Corporate Security withina Corporate Governance Framework

As understanding of the impact of corporate governance oncorporate security is beginning to deepen, concerns have been voicedabout the way in which guiding principles are applied in practice.There are fears that overzealous corporate governance couldundermine rather than strengthen a company's ability to managesecurity risks.
Corporate governance has helped to create a culture that supportsthe furtherance of good and best practice, where information aboutthe most effective types of behaviors, processes, structures andprotocols is shared. Security professionals often describe what they doas 'non-competitive' and rely on regular contact and intelligencepooling with peers in other companies to get their jobs done. A case in point is the bank fraud unit that bring together corporate security managers from various banks in the sector who share information. Thismostly happens informally through the networks or through sector or adhocgroupings. Inevitably, heads of security often have access to sensitiveinformation about other companies, sometimes competitors, which isgoverned by a 'gentleman's agreement'. Although no one could recallan instance of this code being broken, it is possible that this codemight be considered contrary to traditional approaches to corporategovernance.There is also a danger that corporate governance reinforces themisperception that all risks can be managed away.

ENTERPRISE RISK MANAGEMENT AND CORPORATE SECURITY.

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to managerisks and seize opportunities related to the achievement of their objectives. Risk management is simply a practice of systematically selecting cost-effective approaches for minimizing the effect of threat realization to the organization. All risks can never

be fully avoided or mitigated simply because of financial and practical limitations. Therefore, all organizations have to accept some level of residual risks

Principles of risk management

The International Organization for Standardization (ISO) identifies the following principles of risk management

Based on ISO 31000, Risk management should:

1. create value – resources expended to mitigate risk should be less than the consequence of inaction
2. be an integral part of organizational processes
3. be part of decision making process
4. explicitly address uncertainty and assumptions
5. be a systematic and structured process
6. be based on the best available information
7. be tailored
8. take human factors into account
9. be transparent and inclusive
10. be dynamic, iterative and responsive to change
11. be capable of continual improvement and enhancement
12. be continually or periodically re-assessed

Security risk management

Management of security risks applies the principles of risk management to the management of security threats. It consists of identifying threats (or risk causes), assessing the effectiveness of existing controls to face those threats, determining the risks' consequence(s), prioritizing the risks by rating the likelihood and impact, classifying the type of risk and selecting an appropriate risk option or risk response.

Global perspective in Risk Management.

The top 10 risks overall vary in nature, there continue to be concerns about operational risk issues, with five of the top 10 risks representing operational concerns. Three of the top 10 risks relate to strategic risk concerns, with two related to concerns about macroeconomic issues. Six of these risks include:

a) Regulatory change and heightened regulatory scrutiny
For the majority of organizations, this risk continues to represent the top overall risk for the fourth consecutive year. Sixty percent of our respondents rated this as a "Significant Impact" risk.

b) Economic conditions in domestic and international markets
Similar to concerns about regulatory scrutiny, 60 percent of respondents rated this as a "Significant Impact" risk. Interestingly, this was rated as the top risk by both boards of directors

and chief executive officers (CEOs) and ranked among the top five risks for all other executives except chief audit executives (CAEs). That these leaders appear to have uncertainty regarding the global economic climate is an important message.

c) Concerns about cyber threats disrupting core operations

With little surprise, this risk is again a top five concern for 2016, as well as the top operational risk overall and for the largest organizations.

d) Succession challenges and the ability to attract and retain talent

This risk is especially prevalent for smaller organizations (those with revenues under $1 billion), likely triggered by a tightening labor market (though the decline in unemployment rates has been relatively modest), and the respondents' perception that significant operational challenges may arise if organizations are unable to sustain a workforce with the skills and expertise needed for growth.

e) Privacy and identity protection

Respondents ranked this risk as a top five risk concern for the first time in 2016. The inclusion of this risk into the top five is consistent with the increasing number of reports of hacking scandals and growing concern over protecting personally identifiable information.

f) There are growing concerns about the rapid speed of disruptive innovations and new technologies

With the speed of change and the advancement of technologies, rapid response to changing market expectations can be a major competitive advantage for organizations that are agile, nimble and able to avoid cumbersome bureaucratic processes that slow down the ability to adjust to new market realities.

CONCLUSION

Governance, Risk Management, and Compliance (GRC) are three pillars that work together for the purpose of assuring that an organization meets its objectives. Governance is the combination of processes established and executed by the board of directors (BOD) that are reflected in the organization's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organization to achieve its objectives. Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organization's success.

GRC is a discipline that aims to synchronize information and activity across governance, risk management and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps. Corporate Security cuts across these three fields and therefor becomes part of the GRC framework going forward.