ARE COMPANIES IN SRI LANKA APPROPRIATELY GEARED TO COMBAT FRAUD?

Ernst & Young

Introduction

In the global sphere fraud and corruption continue to pose major challenges to businesses today. Following the failures of Enron and Worldcom, Lehman Brothers, Freddie Mac, Fannie Mae and Satyam in high-profile fraud scandals, and the uncovering of the Berni Madoff Ponzi schemes, fraud scandals continue to be reported across the globe. Complex business models, complex product offerings and e-commerce have paved the way for increasingly sophisticated fraud schemes and cyber-crime is largely on the rise today.

❝ While certain frauds may be deeply entrenched in the organization and in its financial system and may never be detected, others may be detected too late ❞

Fraud has multiple facets and could occur by way of misappropriation of assets, by falsification of financial statements and by bribery and corruption and is often committed by the management and employees of an organization. Irreparable damage can be caused to an organization as a result of fraud which if undetected could result in considerable financial loss resulting in crippling or closure of the organization. Financial loss could result from the misappropriation of assets, revenue leakage, loss from corruption, punitive damages arising from non-compliance with regulations on bribery or from business impairment due to damage arising from reputational loss. Moreover, besides financial loss, following the detection of a fraud, the management of an organization would spend considerable time while in the throes of investigating and taking punitive action, whereas its efforts would have been more productively employed in carrying on and enhancing the performance of the organization. Loss of employee morale during the period of the investigation arising from disruption to day-to-day operations and from a perception that management's trust in its employees is damaged and loss of high performing employees are the spin off effects of detected fraud.

Fraudsters often enjoy the advantage of anonymity and considering the insidious nature of fraud, it often lies undetected. While certain frauds may be deeply entrenched in the organization and in its financial system and may never be detected, others may be detected too late. Although the risk of fraud may never be eliminated, organizations are advised to take adequate measures to mitigate the occurrence of fraud, in order to detect and prevent fraud before it causes irreparable damage to the organization.

❝ In Sri Lanka, corporate failures and heavy losses sustained due to fraud have been publicly reported within the past 10 years which resulted in loss of employment for a large number of people, economic loss to shareholders and to the public. ❞

Discussion of the problem

In Sri Lanka, corporate failures and heavy losses sustained due to fraud have been publicly reported within the past 10 years which resulted in loss of employment for a large number of people, economic loss to shareholders and to the public. This paper seeks to understand if corporates in Sri Lanka are sufficiently aware of the business risk associated with fraud and corruption and if sufficient measures are being taken to mitigate the risk of fraud.

Methodology

A survey was undertaken by Ernst & Young through an independent agency where 100 persons were interviewed in Sri Lanka between the period 5th to 23rd February 2015. Interviews were administered face-to-face and lasted on average 15 minutes. The interviewees were selected from companies which employed more than 100 persons, and consisted of 59% male and 41% female. Of the respondents interviewed, 20% were employed by companies listed on the Colombo Stock Exchange, 53%

were from privately owned companies, 8% were employed by state-owned companies and 19% were from the government and public sector.

In terms of level of authority in the company, 16% were from senior management, 50% were from middle management and 34% were employees.

Among the persons interviewed, 44% were between 25 to 34 years old, 29% were between 35 to 44 years old and 22% were between 45 to 54 years old.

Results of the survey regarding a Code of Conduct

56% of the respondents agreed that their organizations had established a formal Code of Conduct.
64% of the respondents agreed that their colleagues complied with the organization's Code of Conduct.
55% of the respondents agreed that the Code of Conduct had little impact on the actual behavior of employees.

Discussion regarding a Code of Conduct

A code of conduct of an organization formally defines and describes the expectations of the organization in relation to employee behavior, the organization's definition of unethical, illegal and fraudulent behavior and serves as a benchmark to measure employee compliance. It is especially useful in measuring fraudulent behavior. While 56% of the respondents agreed that their organizations had established a formal Code of Conduct, it follows that 44% of the companies represented by the interviewees had not established a formal Code of Conduct.

Of the respondents who affirmed that their organizations had a formal Code of Conduct, 64% believed that their colleagues complied with the Code of Conduct while 55% believed that the Code of Conduct had little impact on the actual behavior of employees.

Based on this study, it appears that approximately 36% of employees were compliant with their Code of Conduct whereas 20% had access to the organization's Code of Conduct but their colleagues believed that they were non compliant and 44% did not have a formal Code by which to measure proper and ethical behavior.

Results of the survey regarding a whistleblower hotline

Only 8% of the respondents affirmed that their organizations had a whistle blower hotline to report fraud, bribery or corruption.
75% stated that they were prepared to use a whistleblower hotline to report a fraud if it was available.
41% said that they preferred to report an incidence of fraud, bribery or corruption to an independent third party while 44% said that they preferred to report such incidents to someone within their own organization and 15% said that they had no preference.

Discussion regarding a whistleblower hotline

While 8% of the respondents affirmed that their organizations had established a whistleblower hotline, it follows that 92% of the organizations represented by the respondents had not established such a mechanism.

" A whistleblowing mechanism is by far the most effective method of uncovering fraud "

A whistleblowing mechanism is by far the most effective method of uncovering fraud, which is insidious and often goes undetected for long periods of time due to cleverly crafted methods of concealing them. Traditional methods of gaining assurance about the adequacy of systems of internal control such as internal and external audit, management review of processes and financial data may fail to uncover cleverly camouflaged incidents of fraud and corruption. An organization's employees, customers or suppliers may however have knowledge of these incidents due to direct association with persons engaged with these transactions. Seldom can a fraudster engage in his/her activities in isolation and is often directly aided and abetted by colleagues which although apparent to those who do not directly engage in fraudulent activity will nevertheless refrain from reporting these incidents due to fear of harassment, disengagement or simply because there is no mechanism to report the fraud.

A whistleblower hotline would enable whistleblowers to report their information to the appropriate person/persons who are suitably independent and equipped to respond to this information. In the absence of a hotline, an employee may report his suspicions to his immediate superior officer or to a person of authority who, if involved in the fraud may suppress this information, destroy evidence and harass the whistleblower. A whistleblower hotline with adequate protection for the whistleblower sends a clear message across the organization of management commitment to ethical behavior.

A whistleblower hotline in isolation will not serve the purpose of unearthing fraud and corruption but should be implemented within the context of a comprehensive frame

work of setting the right 'tone at the top', protecting whistleblowers and maintaining confidentiality, having a pre-determined whistleblower response plan which will ensure quick action, and engaging the compliance officer with direct oversight of the non-executive directors.

Results of the survey regarding amending financial reports to provide a more positive outlook on results

The question was asked of the respondents if amending financial reports to provide a more positive outlook on results can be justified if they help a business survive, and 44% of the respondents agreed in the affirmative.

Discussion regarding amending financial reports to provide a more positive outlook on results

It's interesting to note that when the respondents were asked the question if they thought that their organization would be at an increased risk of being a victim of fraud over the next few years, only 21% answered in the affirmative and 62% answered that they did not believe that their organizations would be at an increased risk of sustaining fraud over the next few years. Yet 44% of the respondents agreed that amending financial reports to provide a more positive outlook on results can be justified to help a business survive, which is tantamount to financial statement fraud. The question which can be asked is if there is sufficient awareness in Sri Lanka as to what constitutes fraud and if fraud is viewed only as misappropriation of assets and that modification of financial statements is not perceived as fraud.

The survey revealed that a high percentage of respondents would be agreeable to unethically and illegally modify their financial results when under financial pressure is deeply worrying. Lack of adequate entity level controls to prevent the falsifying of financial information, understanding of fraud risks and adequate process level controls to prevent and/or early detection of fraud is vital.

The Sri Lanka Accounting Standards and Monitoring Board was established with the mandate to monitor compliance with the Sri Lanka Accounting Standards and the Sri Lanka Auditing Standards in the preparation, presentation and audit of financial statements of specified business enterprises. The Sri Lanka Accounting and Auditing Standards Act No. 15 of 1995 and the regulations made under the Act have defined certain enterprises to be Specified Business Enterprises. The Act imposes certain duties and obligations on specified business enterprises and their directors, officers and auditors, the default of which would result in various penalties, extending up to an imprisonment of either description for a term of 5 years.

The Securities and Exchange Commission of Sri Lanka together with the Institute of Chartered Accountants of Sri Lanka published the "Code of Best Practices on Corporate Governance" in the year 2008 in order to establish good corporate governance practices in the Sri Lankan Capital Market.

Results of the survey regarding organizations' preparedness against cyber attacks

When asked the question if the organization was fully prepared to protect itself against cyber-attacks, only 49% agreed in the affirmative, 28% were unsure and 23% believed that their organization was not fully prepared to protect itself against cyber-attacks.

47% of the respondents confirmed that their organizations had provided them with data security training to protect them from falling victim to phishing attacks while 34% had no training and 19% were unsure if they had received training.

Discussion regarding organizations' preparedness against cyber attacks

Today, organizations are increasingly reliant on platforms which are linked to the internet and interconnectivity of people, devices and organizations connected via social media and using cloud technology is a breeding ground of a new brand of cyber criminals and hackers who persistently exploit these new found vulnerabilities.

Lack of preparedness against cyber-attacks is widely viewed as an IT issue and few organizations view it as a business risk. A cyber-attack could pose a major risk to an organization financially when it affects business operations, causes loss or damage to data, financial statements and causes legal exposure with serious reputational damage. Due to lack of awareness and insufficient security training, employees, especially at non-management level are easy victims of cyber fraud. In a phishing attack, a hacker could use targeted emails sent to companies and individuals to extract confidential information or to plant malware which could easily infiltrate an organization's information systems and cause widespread damage.

❝ Today, organizations are increasingly reliant on platforms which are linked to the internet and interconnectivity of people ❞

In order to be prepared for a cyber breach, companies are required to develop a response framework which is robust and involves input from all levels of management, including an organization's legal counsel in order to recover quickly with the minimum damage.

Results of the survey regarding lack of proactive efforts in combating fraud

When asked if the organizations efforts to combat fraud bribery and corruption have been increasing or decreasing in the years 2013 and 2014, 46% of the respondents said that there was no change and 35% believed that there had been an increase in such efforts.

Discussion regarding lack of proactive efforts in combating fraud

Approximately 35% of respondents felt that more effort was being made by organizations to combat fraud. A key aspect of prevention and detection of fraudulent activities is ensuring that employees are communicated to and educated as to what processes are in place and what avenues are available to them in the instance they become aware of fraud.

The remainder of the respondents either did not see a change or felt that the efforts were lower than what it had been in previous years. This may have been due to organizations being complacent as to the probability or fraud or poor communication to employees. In both instances, this leaves the organization more vulnerable to fraudulent attacks as opportunities to commit fraud may not be addressed and employees are then misguided as to how prevalent fraud is, and what measures they need to take to safeguard themselves to rationalizing an opportunity that presents itself

Conclusion

Strong ethical leadership is vital to sustain a culture of ethical business and good compliance which will contribute to long-term sustainability and assist an organization in directing its resources to facilitate business growth. Organizations in Sri Lanka need to strengthen their anti-fraud framework with an organization-specific Code of Conduct, Anti Bribery and Corruption Policy and a Whistleblower mechanism which is well understood by their employees and implemented without exception.

Lack of sufficient awareness of the risks to an organization from a cyber-breach could result in tremendous financial and reputational loss and many organizations in Sri Lanka are yet to understand and respond to this risk with training of its employees and a response plan coupled with other preventive measures.

The results indicate that whilst there is some awareness of what fraud entails, there is an entire type of fraud, such as financial statement fraud that is not perceived to be a risk to the organization. This could potentially lead to a breach of current standards and regulations, with the perpetrator deemed to be the highest echelons of management.

Tools to identify fraud, such as whistleblowing is predominantly ignored in the current context. The lack of access to reporting fraud, results in fraud going undetected over a long period of time; and more importantly represents the stance taken by the organization on fraudulent activities. The tone at the top and the way it manifests itself leads the way employees accept what is appropriate and modifies their behavior accordingly.

In conclusion, whilst the groundwork has been set in terms of basic awareness of fraud, many inroads needs to be made to strengthen both organizations' and employees' knowledge and tools to combat fraud proactively.

“ Lack of sufficient awareness of the risks to an organization from a cyber-breach could result in tremendous financial and reputational loss ”