# Risk management business plan examples

Business, Management

“ No one said that business was going to be easy” is a common statement in the business world. The essence behind this statement is the actuality that business success is not a guarantee. There are possibilities of failure due to different reasons, emanating from both the business process and the external environment (Childs & Dietrich, 2002). Such risks are different when compared along the lines of frequency, likelihood of occurrence and severity. Below are eight risks that most organizations are prone two. These are analyzed in light of a modern organization operating on the global scene as one among the largest retail corporations, Premium Stores Inc.

## Internal Risks

Strategic risk

Strategic risk refers to business uncertainties that are associated with industry within which the organization operates. Speaking of industry, the source of this risk is the competition associated with the industry, as well as the market forces associated with the industry. This may include fluctuations in demand and supply. In responding to this risk, business consultants advise that all organizations should act proactively when assessing an organization (Childs & Dietrich, 2002). Essentially, this refers to proper scanning of the environment using the Porters five forces analysis. After the organization has ventured into the industry, the only response worth putting into practice is creation of competitive advantage. Frequencies of these risks depend on the industry in focus.

## Financial Risk

It is not uncommon for a business to go into financial distress. Why? This is usually because financial procedures and structures of an organization could make it weak to the extent that it cannot meet its financial obligations. The source of the risk in this case is the loophole in the financial structure of the business (Carroll, 2009). While Premium Inc has not been in a state of distress before, all due care should be taken. The response here is thorough auditing and remodeling of the financial structure, with special consideration to technology. These are controllable risks, which can be said to be medium level organizational risks.

## Operational Risk

In Premium Stores Inc, the operational risk is the uncertainty that is part and parcel of the way in which the organization does things. Essentially therefore, the operational risk is part of the structure and culture of the organization. Premium Inc has always endeavored to use up to date technology in going about the different operations within the organization (Childs & Dietrich, 2002). Latest technology eliminates the inefficiencies associated with redundant methods. Operational risk can manifest through the inability of an organization to keep up the pace. The response is simply the restructuring of the processes. The operational risks are extremely common and frequent and highly severe. However, they are the most controllable risks since they are concerned with changes in policy.

## Performance Risks

These uncertainties are associated with the human resource department. They are quite common or frequent but less severe because the organization has control over such risks. The primary response to such risks is the use of motivation and friendlier human resource practices. Premium Inc is known for its unique treatment of human resources. The human resources are referred to Associates. This motivates them to work hard. They are controllable risks.

## External risks

Compliance Risk

Also referred to as the legal risk, the origin of this form of uncertainty is a change in the laws of the country or state as well as the failure to observe such requirements as taxation and garbage disposal guidelines. Being a retail organization, Premium Stores Inc operates in more than 15 countries. The laws of such countries vary greatly. This is the reason why at times, the organization has found itself in court over different issues on illegality. The response to the compliance risk is the creation of a legal department which can elaborate the anticipated legal changes and advise the company accordingly (Carroll, 2009). This risk is frequent and less severe. It is controllable since it is a matter of policy.

## Natural Risks

When Hurricane Katrina hit New Orleans, one Premium Inc store was swept away. Such incidences as hurricanes and floods are among the most

common sources of natural risk. These are quite severe, but less likely to occur. They are seriously uncontrollable since they are natural forces.

## Economic Risks

These are associated with the changes in the economy – especially such macro level changes as inflation and recession. The organization has no control over such changes, but can come up with coping strategies. Frequency depends on the country in which the organization is operating, and the approach the organization uses. For instance, the prices of consumer goods sold by Premium Stores Inc vary from time to time in different countries.

## The Connection between the Strategic Risk and the Global Scene

Apparently, the retail industry is a global industry. Premium Stores Inc, being an organization operating on the international scene, is affected by the variations in the industry defining factors in the rest of the world. Such changes are associated with competitors. As a matter of fact, competition is bound to be more serious on the international scene due to the presence of such organizations as Target Corporation, Kmart and Tesco. What this means therefore is that strategic risk is more frequent and severe in a global industry (Carroll, 2009).

## Business Contingency Planning

Strategic Pre-Incident Changes

Pre-incident changes that a company would adopt include all the precautionary measures in relation to risk. This will help Premium Inc

overcome various risks and challenges in many ways. The most prominent thing in relation to pre-incident planning is identifying and evaluating potential threats. The plan will include mechanisms that evaluate the business environment, both external and internal, with an aim of establishing the existence or otherwise of risks and hazards. Upon identification of the possible hazards, the plan will enable the management to come up with proactive measures that will possibly mitigate the chances of the risk affecting the organization or eliminating the risk factor in totality (Carroll, 2009). Worth noting is the fact that Premium Inc, much like any other organization has no control over external threats. The organization should therefore restructure the vulnerable function of business in such a way that it will absorb the shocks in the event that there is an external threat. Conversely, Premium Inc has full control over risks that are inherent of the everyday operations for instance; an organization has full control over all risks emanating from the human resource department. As such, an organization will use the plan to proactively do away with the unproductive members of the workforce.

In addition to the above, the organization should embrace pre-incident plan to the extent of ensuring stability of resources. BCP helps an organization overcome potential risks by ensuring constant availability of resources. This is achieved through devising reserves as well as buffer stocks. Much like the material stocks an organization can have backup plans in the human resource function. This can be done through staffing in such a way that normal business activities can continue running in the absence of a number of employees. Such changes ensure that the stakeholder’s interests are

catered for despite unfavorable condition in the market. Lack of resources can be a major limiting factor as far as the going concern concept is concerned. Constant availability of resources ensures the business continues operating as a going concern into the foreseeable future (Carroll, 2009). Such pre-incident changes will uphold shareholders confidence attracting more potential investors since the average investor is risk averse. Resource availability is a key element in the business contingency plan, more so, in a manufacturing concern. This is especially so when the resources concerned is material in nature.

## Ethical Use and Protection of Sensitive Data

A business will always have information that is considered sensitive. Sensitive data is any form of raw information whose alteration can cause serious deviations from the course towards the attainment of long term goals of a business. Apparently, the most sensitive data relates to financial activity and the human resources records of the business. Worth mentioning is the reality that an organization holds personal information which must be handled ethically. Ethical handling of such information refers to the access of the records by only the persons that are allowed to handle such information (Childs & Dietrich, 2002). For instance, no other employee should have access to the human resources databases to view the portfolios of other employees, except the personnel manager. Similarly, other employees are not supposed to access such sensitive financial data as the payroll and so on, accepts the accountants and the auditors. Ethics further dictates that those who have access to such data should not reveal to other unauthorized parties. While this is the case, the business is under obligation to protect

such sensitive business data from two things – access by the unauthorized parties and the damage that may be caused by such disasters as fire. Such protection can be done through physical controls such as locking the records in strong safes or use of technological controls such as cloud computing and the use of one time passwords.

## Ethical Use and Protection of Customer Records

An organization cannot be in operation without relevant customer information. Ethically speaking, customer information should not be accessed by all internal stakeholders. As such, the organization should seek to establish mechanisms to limit the access to the relevant parties only, locking out all unauthorized parties. Similarly, the organization should seek to protect such information through backups, just in case a disaster occurs. Back-up information systems are the most effective form of protecting the information. Making backups ensures continuous operations take place as far as transactions and decision making is concerned. Information stored by an organization relates to important records such as customer transactions as well as all dealings with the creditors. Such information is particularly important as it relates to credit management – an essential part of large scale transactions (Seese, 2010). By creating backups business contingency management ensures that such information is continually available to be used in making critical decisions and transactions.

## Communication Plan to Be Used During and Following the Disruption

The period during and after the occurrence of a major disturbance is a time when the need for information and adequate reliable communication is

immediate. The reason why such information and communication is immediate is because the major stakeholders both from within and without the organization seek information on the clarification regarding the future of the relationship between such a stakeholder and the organization. The main stakeholders interested in such information are: the customers, the suppliers, the employees, the shareholders, the government, the local community and the media houses (FEMA, 2012). The regulators and potential investors will as well be interested in understanding the future of their relationship with the organization. While this is the case, the organization will have to come up with a comprehensive communication plan – comprehensive in the sense that it addresses the information needs of all the above mentioned stakeholders.

Such communication will perfectly be attained through a plan that is coordinated by the crisis communication center. The crisis communication center is an emergency unit that disseminates information to the relevant parties in a timely manner. This unit works both during the crisis and in the post-crisis period. Worth noting however, is the reality that, depending on the severity of the phenomenon, the unit is especially functional after the crisis. The communication plan is depicted in the figure below.

Figure 1: Crisis Communications Hub & Spoke Diagram - Text Version

Source: (FEMA, 2012) http://www. ready. gov/business/implementation/crisis

## Restoring Operations after the Disruption Has Occurred (Post-Incident)

Restoration of the organizational operations is, arguably one among the most difficult phases of dealing with crisis. Restoration, which entails a

multistep process, may be too costly depending on the extent to which the damage was done. Apparently, the multi-step process is designed in such a manner that there is a timeline to be observed for proper sequencing and recovery of both the physical state of the organizational facilities and the operations of the organization (Rick & Francine, 2004). The ultimate aim of the organization is to restore the pre-incident organizational climate. The process of the recovery follows the following phases:

## Crisis Phase

This phase is associated with the first few hours of the incident. Usually, this phase is associated with a period of between 24 and 48 hours. During this time, the major activities are all those revolving around the evacuation, rescuing of people and property. During this phase, very little is done to estimate the loss because the evaluators will still need to ascertain the worth of every part affected by the disaster. During this phase all the affected stakeholders are reassured of their stability.

## Planning Phase

The second, phase, which comes immediately after the crisis phase, entails in-depth planning for the re-organization of the departments and all other parts of the organization that are affected by the crisis. It is important to mention that this phase covers a period of between 48 hours and 30 days. The main concerns of this stage revolve around the restoration of the pre-incident crisis (Rick & Francine, 2004). The fact that planning is a continuous process explains why the phase takes a little longer. The planning phase deals with the reinstatement of the economic stability of the organization,

the strengthening of the communication channels and the reinstatement of the perceptions of the organization by the community.

## Rebuilding Phase

This phase begins at the 48th hour after the incident occurs and goes on for approximately two weeks. The main concerns at this stage involve the reconstruction and refurbishments of the buildings and other resources such as buildings and machinery (Malecki & American Institute for Property and Liability Underwriters, 1986). Similarly, realignment of the organization's operations is done. Realignment touches on all departments, ranging from the common operations to the human resources department.

## Ongoing Recovery Phase

Ongoing recovery is quite essential in the sense that the organization will resume its business activities, while the process continues. The organization will be running as the management invests in the revival of other parts of the organization (Rick & Francine, 2004). This phase begins immediately after the crisis to a point referred to as full recovery. It entails remodeling of the business structures and internal systems.

## The Implementation

Implementation of the plan for Premium Inc will take into special consideration the security of the information, and the backup systems associated with information technology. The plan will, therefore, give prominence to back up systems and the use of limits in the access of information and databases. The plan will therefore be implemented all through the business operation period. What this means is that the backup

system will be continually updated to reflect the latest information. With regard to backup systems, the plan will; employ such features as cloud computing, which will see information stored in online databases where it can be retrieved easily in the event that havoc occurs.

The pre-incident plans can be made and implemented at all levels of management as well as in all organizational departments. It is important to mention that in the pre-incident implementation, the organization should give prominence to the decision to involve all employees, so that they can be aware of what is expected of them in the event that the organization is stricken by disaster. Similarly, the implementation process should embrace such professionals as the valuation and the risk management gurus for purposes of estimating the anticipated losses through such approaches as the expected monetary value (EMV) and the expected opportunity loss (EOL) (Malecki & American Institute for Property and Liability Underwriters, 1986). What happens when these people are used in an organization is that the organization established the exact amount of money required in the implementation process. The most important thing is that the implementation should be an ongoing process so that if havoc strikes at any one time, information secured in the backup will be up to date.

## References

Carroll, R. (2009). Risk management handbook for health care organizations. San Francisco: Jossey-Bass.

Childs, D. R., & Dietrich, S. (2002). Contingency Planning and Disaster Recovery: A Small Business Guide. Hoboken, NJ: John Wiley & Sons.

Federal Emergency Management Authority. (2012). Crisis Communications

Plan. Retrieved from: http://www. ready. gov/business/implementation/crisis

Malecki, D. S., & American Institute for Property and Liability Underwriters. (1986). Commercial liability risk management and insurance. Malvern, Pa: American Institute for Property and Liability Underwriters.

Rick, A & Francine, T. 2004. A model of organizational recovery. Journal of Emergency Management, Vol. 2, No. 1. Retrieved on 9th august 2013 from: http://www. managementcontinuity. com/images/Allen1. pdf

Seese, M. (2010). Scrappy business contingency planning: How to bullet-proof your business and laugh at volcanoes, tornadoes, locust plagues and hard drive crashes. Cupertino, CA: Happy About.