Security and risk management

Business, Management

Risk can be closely linked with the existence of humans on planet earth, as they continue to identify a number of sudden or in some instances unexpected events. These events can be classified as either natural or possibly even man made. The difficulty of avoiding the uncertainty of the consequence related to the risk, in the long term makes people risk adverse. Taking into consideration risk avoidance, risk transfer, risk retention and where appropriate the necessity of risk reduction, by reducing the impact of the event from initially occurring.

The risk management model has been around for many years and can be seen as one of the oldest human activities. Documented within the bible it identifies Noah, who built the ark and managed the crisis of the flood. This clearly shows how Noah can be expressed and be seen as one of the earliest contributors towards risk management. According to (Borodzicz, 2005 p2) the spoken words of Aristotle, " It must be expected that something unexpected must happen", is another figure that can be identified as having an understanding in the importance of risk.

As there are four core strategies that fulfil the concept of risk management, it should be made aware and taken into consideration that risk management is a subject that is concerned with the overall management of a company's activity. When selecting any risk management strategy to be used within the organisations environment, the management process should concentrate on initially identifying the risk that needs to be managed. This is then followed with the evaluation or assessment of the risk, to determine what extent in terms of impact the risk has on the organisation and the probability of the risk occurring.

The business can then plan and manage the risk using the core strategies. Risk occurrences cannot be managed without identifying what the risk is and assessing the severity and likelihood of it occurring. The information gathered during risk identification and evaluation will identify the specific strategy or strategies to manage the risk. When considering risk management it has been identified and evaluated that risk could require a particular strategy or a mixture of various strategies. (Conti, 2012) states that the key strategies involved in the concept of risk management are identified as Avoidance, Transfer, Retention and Reduction.

Main Body Risk management is defined by (Hubbard 2009 p46) as the identification, assessment, and prioritisation of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative). Followed by coordinated and economical application of resources to minimise, monitor, and control the probability or impact of unforeseeable events. Risk management involves the utilisation of techniques in order to arrive at cost-effective strategies within the organisation that will not harm the objectives of the business.

Risk Avoidance Risk avoidance is eliminating risk by avoiding it. It is a risk management strategy on not performing an activity that could carry a risk. An example would be for somebody not to purchase a security business in order to not take on the legal liability that comes with it. Another example would be not flying, in order to not take on the risk that the airplane could be hijacked. Avoidance may seem the solution to all risks, but avoiding risks means losing out on the potential gain that accepting the risk may have allowed.

Being involved within a security business to avoid the risk of loss also avoids the possibility of earning profit for the business. It is a risk management strategy on not performing an activity that could carry a risk. (Borodzicz 2005) argued that risk can hardly be completely avoided especially if the work of the organisation is of a sensitive nature and carries a risk on its own, risk avoidance may not be a strategy to be considered. The risk avoidance strategy is very often used to manage high impact risk, with high probability the risk with the greatest loss and the greatest probability of occurring.

Those risks with lower probability of occurring and lower loss are likely to be managed by risk transfer or risk reduction. Risk Transfer This strategy involves the transfer of risks from one organisation to a third party. This is usually achieved through sub-contracting to other organisations, where costs can be extremely high. Risk transfer has been and continues to be a strategy where the risk is found to be difficult to reduce or avoid. In countries where war is present the risk of assassination of both UN workers and aid workers is evermore present.

According to (Kingston & Behn n. d) lives of workers have been lost as a result of criminally motivated killings. This has led to the United Nations subcontracting many activities of local aid organisations who serve as partners on a vast amount of projects. Sub-contracting has cost implications for affecting the organisations standards. If standards are not set by organisation before the third party becomes involved, it can result in terrible consequences. Poor practices, underperformance and compromising of standards by the third party to carry out the activity are likely to be outcomes of the situation. Risk Retention

Risk retention strategy aims to retain risks that could not be avoided or transferred to a third party. Risk retention involves being able to accept the loss, or benefit of gain, from a risk when it occurs. Risk retention is an ideal strategy for small risks, where the cost of insuring against the risk would be greater over a set amount of time than the total losses sustained. Risk retention may in some circumstances be acceptable if the chance of a very large loss is small. A security company might decide to retain 4 security officers instead of increasing its security officer numbers.

The security manager has evaluated that there is a low impact risk with low probability for anyone to enter the premises as there is an external security company patrolling outside. The security manager has identified, that the cost of employing extra officers or even subcontracting to another security company would be far too high and would not be cost effective. Usually an organisation retains risks that is seen as minor or the sources of which are usually internal and within the control of the organisation.

It has been noted in (Charrel and Galarreta, 2007) that the risk retention strategy involves doing whatever is needed to reduce the risk. “ It comprises steps taken to reduce either the probability of an event occurring or the financial impact if the worst happens”. Risk Reduction Risk reduction involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, a sprinkler system within a building is designed to put out a fire and to reduce the risk of loss by the fire. This method could cause a greater loss by water damage and it may not be suitable for the situation.

Acquiring Halon fire suppression systems may mitigate that risk, but the cost may be impossible as a strategy. Having a functioning CCTV system, locks and reinforced access control systems such as turnstiles within the building reduces the likelihood of a possible crime being committed. Having necessary protocols and sound procedures in place strengthens the overall protection of the business, limiting the likelihood of a security concern to become present. A possible situation could be when the risk of burglary and forced entry is assessed as high impact and of a higher likelihood.

Target hardening by building high walls with barbed wire and employing a security guard company to monitor the premises can all form part of a wider risk reduction strategy. A risk reduction strategy may not eliminate all of the risks identified but instead, it aims at reducing the impact and likelihood of the risk from evolving with other possible interventions if the risk was to reoccur. Conclusion The four strategies involved in the concept of risk management are risk avoidance, risk transfer, risk retention and risk reduction.

The choice of strategy should be based around the various stages of the risk management process. A thorough risk identification process should be orientated around identifying and reviewing all possible risks that the security organisation has been exposed to. Information can be gathered from various sources both within the business and outside of the business. Being able to consider a risk evaluation is important, analysing the risk by measuring what impact the risk has on the security company and the likelihood of the risk occurring.

The selection of the required risk management strategy depends on the results of other risk management processes. This determines the necessary course of action for a specific strategy to successfully deal with the risk. Risk management strategies can be effective if new risks are identified when they become apparent. Risk monitoring and control should be a continuous process allowing risks to be identified and evaluated in order for a strategy to be in place to manage the risk. Risk control is an important action taken by security companies as it is established to identify, manage and reduce or eliminate risks.

Risk control is very important to security companies as it allows information gained during a security risk assessment to be developed and where necessary changes applied to control the risks. Risk control can involve implementing new security site specific standards, polices and company procedure changes that can reduce or eliminate certain risks within the company. Having a sound policy on risk reduction and elimination should be taken into consideration by any security company. All risk management processes should prioritise risks with high impact and identify which risks are most likely to occur.

Risks that could possibly threaten the existence of the security company should take precedence. Security companies should be aware not to ignore low impact or low possibility risks as there is the possibility that these risks could lead to high impact risks in the long term. ISO 31000 confirms this, as it continually monitors risk management and the overall risk management process. ISO 31000 aims to be able to review risk management by taking into consideration policies, risks, controls and the overall assessment process.