Security and risk management helps organisations stay safe nhs

Risk management has become an integral part of business structure. Looking at the way businesses are operated nowadays, understanding the concept of risk management will help risk managers and organisation managements stay safe. It also goes a long way to fulfil the law including the statutory risk assessment that must be carried out by every organisation under the Management of Health and Safety at Work Regulations 1999. It might save organisation some of the wasted resources as well. There have been various assumptions about organisation failures and disasters in which some theorists believed in events being natural, some believed and have explained them using the knowledge of science and some believe they are fundamental that some things must go wrong. In the modern days, major risks failures are now being seen as human error rather than acts of God as previously perceived. (Reason, 1990). They are as a result of failed communication (Irwin, 1995; Drottz-Sjoberg, 2003). It was supposed by Pigeon that risk is as a result of cultural misunderstanding (1992). In a nutshell, there are still a lot to research into in the area of risk management in order to fully understand and agree on a single concept of the causes of risk and management. Scientifically, events happen by chance and the likelihood of it happening is termed probability.

Security risk has gained a wider and heightened view considering the current domestic and international security in our society. Every facet of life does have an associated security risk which determines both the success and failure of our set goals. It was observed by Douglas that risk is not just a 'thing' but a way of thinking and that not just the chances or probability of an event occurring but the 'magnitude of its outcome' (1992: 31). It is an all-

encompassing feature of modern life to think about associated dangers with risk (Beck, 1992). There have been several definitions of what risk management means to various theorists and researchers. Amongst the definitions is;

".......... a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself. Risks as opposed to older dangers are consequences which relate to the threatening force of modernisation and to its globalisation of doubt" (Beck, 1992: 21).

Risk has been explained by Clive Smallman as a way of communicating series of futures events which are conceptually uncertain and vary through accessible data and the modes of argument (1999). In the course of this essay, three different forms of risk that could face the Security Manager of an organisation shall be considered. This essay shall look into Health and Safety risk, financial risk, and Service quality risk. Correlations and dissimilarities of these risks shall be considered in relation to health services. However, various ways of dealing with these risks shall be looked into in Leicester Royal infirmary. Surveys have shown that vast majority of organisations fell below the expected business risk assessment and control standards expected of them which implies that they might be susceptible to business risk should there be any major attack on these organisations (Clive, 1999)

Effective risk identification and management is dependent on knowledge management. Research have shown that the whole philosophy of knowledge management is based on the hypothesis that knowledge develops through a

social process, where individuals share implicit and precise knowledge (Nonaka et al 1995). However, the conversion of knowledge may be achieved through the experiential learning cycle (Kolb, 1996). There are needs for the Security Manager to always involve themselves in skills and knowledge acquisitions and development that would enable them discharge their duties effectively and efficiently.

Risk being a major threat to organisation's sustainability and profitability cannot be handled with levity. Knowledge and skills management is very much the modern universal panacea, and its application in risk management has already started. Analysis of securities trading failures at Barings, Kidder Peabody and Metallgesellschaft Refining and Marketing, has revealed that the value of knowledge management and its transfer to decision makers, have an important role to play in organisation's sustainability. However, it is good for organisation to keep testing the level of embedding knowledge periodically to check for knowledge gaps rather than waiting till when there is major system or process failure. (Marshall et al, 1996)

Regardless of risk management understanding, there are some barriers to effective risk management which organisation needs to overcome for the continuity of their business. Culture and trust is one of the important factors whereby senior management must always be ready to adjust organisational culture in response to environmental changes. Organisations need not to absolutely decline public opinion and expert advice as it affects their organisations. In every information, there could be an element of truth. Trust is a key factor in risk management which need not to be undermined

(Pidgeon, 1999). Risks have to be communicated effectively in order for it to be meaningful.

"................. Recent high-profile failures to communicate risk adequately, and notably in the public health arena, have led to an increasingly sceptical public" (Beck, 1992).

Organisation should desist from using ambiguous statements to mislead the public and minimized perceived risks. Such behaviours lead to organisations failures (Gouran et al, 1986)

Another common barrier to risk communication is proper information handling. How effective an instruction is carried out is a function of how the information communicated is received or perceived (Bella, 1987). Various levels of information are needed to communicate different hazards and if this is not fully and effectively handled, concerned parties find it difficult to fully understand and handle the complexities of ill-structured problems. A failure to properly interpret information may also lead to the failure to see or appreciate the magnitude of some emergent danger (Reason, 1990). However, there are situations where the hazard indicators are recognised but undermined. Undermining the risk potentials is hazardous (Quarantelli, 1988). Risk, being a social construct could be difficult to communicate and accept sometimes because of its nature. It is full of probability and uncertainties. The level of damage a risk may pose on individuals or groups or organisations is based on human judgement. Major cause of risk miscommunication is non expert interpretation of terminologies (Tonn et al 1991).

" In attempting to compare potential interpretations of terms such as 'safe', 'acceptable' and 'tolerable', experts face a 'semantic minefield'" (Fisher, 1991). The intricacy in risk communication is not far from the fact that people tend to use similar terms in different ways, and as such different terms to denote similar meanings (Tonn et al, 1991). There has been a question that can risk be assessed? However, it is now a statutory requirements for every organisation and is even a criminal offence for not having it done as and when due. It is essential that organisation carry out periodic risk assessment in order to plan ahead and meet statutory requirements (Kovacich et al, 2003). It is part of the duty of government to ensure that all citizens are well protected likewise their properties which in turns reduce their likelihood of being victims of crime. (Sandra, 1999). Turnbull report of 1999 on Internal Control, Guidance for the Director on combine code has removed the doubt about whose responsibility is the risk policy formation and management in organisations.

There is always a need for a risk Manager and some organisations may term it Health and Safety Officer or Manager. Their main responsibility is to assess the risk that could face the organisation and determine what action should be taken in line with the organisation policy which could have been drafted by the Directors. Risk assessment can be divided into five stages in order to make the process simple for the risk Managers; The first step is to Identify the hazards; while the next two steps have to do with deciding on who might be harmed or at risk, how is it going to happen, evaluate the risks and decide on precautionary measures that should be taken. On the other hand, the last two stages have to do with recording whatever findings that have been

made, implement actions, carry out the assessment review and update if necessary (HSE, 2006).

" Risk management strategy refers to the implementation of all those measures necessary for determining a reasonable and acceptable level of corporate risk, and then for managing corporate activities so as to avoid exceeding that level" (McCrae et al, 2000). It was explained further by Michael McCrae that there are four major phases in risk management. It is important for the risk to be identified in line with the nature of the organisation's business; the likelihood of its occurrence has to be analysed with its impact and timing on the organisation's business. Once these are established, there is need to plan on how to curtail the risk within a reasonable and acceptable limit as stated in the company's policy as a guide to planning and process implementation.

Although, there is a simpler risk management structure suggested by Alexander (1993) which is useful in support service operations. By combining this structure with that of Boon's (1998), there are seven stages in which the first four stages fit into Alexander's structure. The first four stages have to do with establishing the framework of risk which is the organisational and risk management strategy within which the rest of the process will occur; establish the criteria against which risk will be assessed and define the structure of the analysis. Identify risks, analyse the risks in terms of its possible effects and the enormity of business disruption and quantify the risks. The second phase involve assessing and prioritising risks by measuring estimated levels of performance risks against the established corporate decision-making criteria, to determine whether the risk is acceptable or not.

Risks have to be treated by accepting and controlling low priority risks; while specific management plan should be developed for other risks. Performance of the risk management system and changes that might impact on it must be monitored and controlled on a periodic basis.

Meanwhile, risk can be categorised into speculative (entrepreneurial) and pure risk (Insurable). Insurance companies have now believed that organisations should work with them in controlling the pure risk rather than leaving the entire risk to insurance companies without putting in place measures that could either avert or reduce the damages in case of any eventualities.(Borodzicz, 2005). Amongst the risk facing organisation is Health and safety risk. It is required by law that an employee be provided a safe place to work. Under the Section 2 of Health and Safety at Work Act 1974 (the HSW Act 1974), " It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees". However, it went further under section 7 on the General duties of employees at work to explain the duty of every employee while at work as thus;

"............. to take reasonable care for the health and safety of himself and of other persons who may be affected by his acts or omissions at work;" and

"............ as regards any duty or requirement imposed on his employer or any other person by or under any of the relevant statutory provisions, to co-operate with him so far as is necessary to enable that duty or requirement to be performed or complied with" (HSW 1974 s7).

Moreover, Management of Health and Safety at Work Regulations 1999 also provides that every workplace require risk assessment and put in place a plan to control all the pure and perceived risks. It is there important to note that Health and safety at work is a joint responsibility of both the employer and employees. Although, there might be a knowledge gap on the part of employee and this shall be dealt with in this essay under the ways of dealing with the risk by the Risk Manager. Amongst the health and safety issues identified in Leicester Royal Infirmary are; Knife stabbing, Syringes and needles, staff assault at car parks and smoking sheds, Mental Health patients getting agitated and aggressive towards staff during treatments and observations, staff sustaining back injury while lifting patients, wet floors and tap leakages, risk of dementia patients walking off from wards etc. Following the risk management process as explained by Michael McCrae, these itemised risks have to be analysed in line with the facilities available to render health and care services in LRI to enable an appropriate plans and strategies be put in place.

It is a statutory requirement that every employer displays a current insurance certificate as required by the Employers' Liability (Compulsory Insurance) Act 1969. In addition to that, it will pay off if employer provides free health and safety trainings for employees on a regular basis so that they know what types of hazards they may face while discharging their duties and how to deal with them in the course of their work (HSE, 2006). Manual handling of patients should be carried out in pairs, though equipments like hoists should be made available. Other ways of dealing with these risks include proper lightings at the car park, human surveillance, and installation

of CCTV to apprehend offenders which could also serve the purpose of crime deterrents (Smith, 1987). However, there should be a dedicated ward or patients' waiting or assessment area for those who have been known with history of aggression or Mental Health related conditions. The area should be manned by human surveillance in an addition to CCTV cameras. In addition to the above, CCTV at the car park increases the tendency of it being used as users believe that they are safe from Victimisation and assaults (Tilley, 1993).

There should be signs to indicate wet floors with a disclaimer clearly written on them in every wet area or where cleaning is in progress. Meanwhile, it is more cost effective to have the confused patients tagged by the use of monitoring or security tagging devices. These devices alert the security or duty staff once the patient approaches the exit door. By so doing, it saves the management the hassle of incident reports while Police / Security staff time can be used for other issues.

Financial risk is another major challenge that managers in organisation could encounter. Various departments have their budgeted allocations at the beginning of their financial year. Majority of the organisations have seen security departments as cost centres because of the capital outlay required in setting up the department, purchasing CCTV and other equipments rather than seeing it as an integral part of their organisations in working towards achieving low shrinkage, lowering costs of production and operational downtimes, enhanced sales returns, increased turnover and profits. (Bamfield, 2005; Kaplan, R. S. and Norton, D. P, 1996). Although, security data are often not timely which could make it difficult to obtain the impact of

appropriate and depict the cost-benefits of funding security strategies by organisations (Howell and Lehockey, 1997). Most organisations tend to outsource Security management department because of the financial implication and the legal process that is involved in case of any major mayhem or incident.

NHS, being a bespoke sector cannot afford trial and error and as such, some of the executives prefer handling their non-clinical departments themselves rather than outsourcing to external management companies. Reason being that it is difficult to manage and monitor the set standards through the outsourcing agents (Howell et al, 1999). Although, this can lead insecurity through improper information, working relationship with other arms of the business like finance, infection control, patients' information management, etc (Adnett et al, 1995). However, in Leicester Royal Infirmary, some of the tasks both clinical and non clinical have been outsourced to Contractors and Facilities Managers like Serco FM. However, NHS has line Managers who oversee the activities of these agents to ensure that they carry out their operations in line with the Trust's guidelines and their performance are reviewed periodically. There is always a need to justify to the NHS Trust why and the cost benefits of every financial resource spent on Security department in terms of infrastructure acquisition, replacement costs of equipments and other project costs.

Periodic auditing of security departments is essential to account for security gap. In as much the security strategy must support the organisation's strategy (Kovacich and Halibozek, 2003), the organisation and the environments of operations must be audited by the security Managers to

ensure that every electronic equipments required and manpower required by him for operations are in place to ensure safety of property, customers and staff members. Security audits consist of two features. One of the features audit the current Security Strength and weaknesses of Management, staff, technologies, processes, procedures and reporting system while the second features have to do with auditing the threats and opportunities in the department, the organisation under review, its actual and intended environment within a short and long term period (Kovacich and Halibozek, 2003., Fisher and Green, 2003). This will also enable the security manager determines the financial needs of the department.

Nevertheless, security departments should be pro-active rather than re-active and the security Manager should embeds security into the process, systems and other departments working practise. By this, security Manager would be seen as part of the structure rather than a necessity or a necessary evil (Kovacich and Halibozek, 2003). This will change the perception towards security team and managements. Amongst other financial risks that could face the Security Managers are price competitions during equipments acquisitions, service or contingency cost uncertainty and economy (national and international). Other financial related risks are working capital, profit margins in relation to savings on the available funding for security operations, return on capital employed and insurance liability costs for all the equipments and man powers employed.

Service Quality is another risk element that requires management attention in any service organisation. Organisations are faced with challenges of managing employee from selection process all through till when the

employee resigns from the organisation. The service delivery quality is a function of some factors to include employees' attitude to their job. There is need for an organisation to have zero-tolerance policies which should be enforced so as not to expose the organisation to future challenges resulting from employee who acts, or threatens to act, violently at work (Johnson, 2000; Perry, 2000; Rolnick, 2000). This has been very important as most of the poor service care issues can be traced to employees' attitudes and behaviours or reactions to management processes. Although, management culture has its own role to play in service quality.

There have been various researches into service quality and 'Servqual' approach was provided by Parasuraman and his colleague as a measurement approach to service quality through identifying ten dimensions of service quality as stated thus: security; communication; access; courtesy; competence; credibility; tangibles; responsiveness; reliability; and understanding the customer. The Servqual instrument measures customers' perception of the service received in relation to their expectations which are based on word of mouth, advertisement and previous experience. (Parasuraman et al, 1994). It is important for employee to have in mind and do unto others the way they want people to do unto them. If this habit and culture is cultivated by every employee, the way they react and attend to their customers will be professional and portray the image of the organization well in the public.

In NHS Hospital such as Leicester Royal Infirmary, customers include patients, staff, patients' relatives, visitors, suppliers and everyone on the premises for any reason whatsoever. Employees should be educated to

understand why they are at work as their existence at work depends on these customers. In 1990, the NHS trust became a corporate business entity which is legally accountable for its own business continuity, clinical negligence and operational failures. NHS and its outsourced units since then owe duty of care to their service customers (Okoroh et al, 2002). In order to deliver an effective customer service by the NHS and its outsourcing agents, policies on the expected standards have to be made available to both staff and public. This will enable employees know what are the expectations of the employer and the public. However, a periodic review through questionnaires and assessments could help in monitoring employees' performance in line with the set standards and if they are not delivering up to the expected standards, refreshers trainings should be organised as a way of reminding them of the contractual agreements they signed with the organisation which has to do with working in partnership with the NHS Trust.

In order to manage risk in NHS hospital, risk control can be broadly classified in three; risk can be reduced, retained or transferred to either the insurance or an outsourcing agent (NHS Estates, 1997). Looking at the various risks discussed above, financial risks can be reduced through the introduction of Private Funding Initiatives (PFI) and Public-Private Partnership (PPP). These will reduce public expenditure and to reduce public (Johnson, 1997) and would also enhance business 'efficiency, economics and effectiveness'-Akhlaghi's 'three Es' (1996). It allows private organisations and individuals to invest their fund in the business and contribute meaningfully to the growth of the business. Employees' orientation could be changed through this approach and make them deliver effective service. This would probably

reduce the risk posed by service quality and Health and safety while the NHS board would have more time dealing with other business areas like management than the provision of service. However, it is very important for the NHS trust be actively involved in the management of the business in order to protect the organisation's integrity, have some level of control, and avert the risk of economical and healthiher service delivery. (Szymanski, 1994; Milne, 1994; Maddock et al, 1998).

In conclusion, amongst the various risks that could face the Security Manager in hospital environments are financial risks, Health and Safety risks and Service Quality risks. These risks affect customers as have been detailed in the course of this essay. For instance, where there is no funding for a Security Manager to put in place some crime control and reduction strategies in the hospital, customers will be victimised and this will impact on the organisation's Health and Safety and poor working environment. Poor training of employees will also invariably lead to poor level of service care as opposed to the expectation of the public. This implies that these risks are dependent on one another and none of them should be undermined. Ultimately, they are all dependent upon adequate funding for the security department.

On the other hand, employee's readiness to be trained and commitments are also important. If resources are available and the employees are not committed or ready to un-learn and re-learn good practice, it will be difficult to make changes to the current process. Though, if the finance risk is addressed using the PFI and PPP, some elements of Health and safety risk such as accident at work, thefts etc can be transferred to insurance

companies and the onus will be on the Security Manager to work with the

management should there be any claim or needs to provide justifications

and protect the organisation against any legal action.