Abstract

The paper critically reviews a case study titled ‘The case of the London ambulance service computer aided dispatch system’ by Davis, 1995. The paper aims to identify two issues regarding this case study: a- ineffective risk management practices by the organisation responsible for implementation and deployment of an information system and b- ineffective leadership style. The paper has been written on assumption that ineffective risk management and leadership style was one of many other factors responsible for the failure of the examined information system. The paper concludes with making recommendations for improvement.
<table>
<thead>
<tr>
<th>S.no.</th>
<th>Content</th>
<th>Pg. no.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>1.1</td>
<td>What is risk management and what is its significance in an organisational context?</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Critical analysis of the case study titled ‘The case of the London ambulance service computer aided dispatch system’ by Davis, 1995.</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>Application of theories to explain the ineffective behaviour of key individuals and groups</td>
<td>6</td>
</tr>
<tr>
<td>2.2</td>
<td>Identification of actual leadership process / style and that which was really needed in this situation</td>
<td>8</td>
</tr>
<tr>
<td>2.3</td>
<td>Explanation of what went wrong and what support is further needed to strengthen the organisation’s ability to cope with the risk</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Appendix</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>References and bibliography</td>
<td>15</td>
</tr>
</tbody>
</table>
1. Introduction

1.1 What is risk management and what is its significance in an organisational context?

Risk is defined as the probability of occurrence of an incident that may result in loss caused to the subject (Kammen and Hassanzahl 2001). In a business environment, the subject is the organisation / business. Business risks are inevitable and businesses operate in the environment that nurtures risk (Barole 2000). Having said so, the internal and external environment of a business has been transformed in such a manner so that risks are inherent. As an example business functions are integrated so that all functions work together and towards a common business goal. Moreover, businesses have to establish persistent communication with its business partners and stakeholders so that they are well-informed of business conduct (Boswell 2001). These practices require support of information technology (IT). This further means that enterprises today are actually a network of inward and outward flow of information and communication which invites several business risks at the same time that may result in creating loss to the organisational assets. These losses can be experienced in the form of loss of data / information, security breach of information, intruders and hackers etc. entering in to the organisational infrastructure with bad intent causing physical damage and or logical damage to the property of business, loss of business reputation and credibility and so forth.

In order to secure the organisation and organisational assets; tangible and intangible both, practicing a management discipline called risk management ensures that the risks inherent to the business and in its external environment can cause the magnitude of damage to the
organisation that is acceptable (COSO 2004). It should therefore be noted that the concept of risk management suggests that risks can be either: a- mitigated or b- transferred. Risk can’t be eradicated, therefore if the cost of risk mitigation and risk transfer exceeds the loss that the risk occurrence may cause then the discipline of risk management suggests the business to live with the risk. European Foundation of Quality Management (2005) defines risk management as the systematic use of process of identification, evaluation, management, and monitoring of risk across the organisation. The information collected as a result of this process is further used to secure, release, and generate value for the organisational assets.

Risk management gains its significance due it benefit outcomes associated with it such as a- securing the organisational assets (tangible and intangible both), b- providing cost-effective solution, c- monitoring and managing risk and d- evaluating and analysing risk. Through adopting effective risk management practices, businesses can ensure to complete their projects within time, enhanced business initiatives such as strategic planning through cost effective solutions, resource optimisation, reduced cost of doing business through mitigating risk and risk factors, development of vigorous contingency plan (Rees and Allen 2008) and so forth

The literature on risk management strongly recommends risk management practices to be adopted by the businesses due to their volatile internal and specifically external environment (Holmlman and Forrest 1991; MGrew and Bilotta 2000; Neef 2005; Mikulecky 2008). The literature further postulates that the impact of risk occurrence varies from organisation to organisation. As an example the unavailability of company information for a period of two hours can be a disaster for a multinational bank whereas a management consultancy firm can tolerate the same situation without any significant losses. Therefore, it is subject to the nature of business that can ascertain the magnitude of impact of risk occurrence. Talking on a very broad and generic spectrum of business context, risk occurrence can be evaluated as business disruptions, incident, catastrophe and disasters. Business disruption can be explained as loss of data or non availability of data, incidents can be explained as false fire alarm which required evacuation of office premise for an hour or project failure etc. A catastrophe or disaster can be explained as loss of human life, major failure of business investment etc.
In order to put the learnt theory into practice, the paper now aims to examine a case study titled: ‘The case of the London ambulance service computer aided dispatch system’ by Davis, 1995. Therefore, the objectives of this paper have been identified as follows:

1.1 Identification of real world situation where a disaster / catastrophe occurred due to failure of preventive controls or failure of risk management.

1.2 Explanation of the ineffective behaviour of appropriate personnel through application of four domains of COBIT framework (plan and organise, acquire and implement, deliver and support, monitor).

1.3 Identification of leadership style required for the situation when the risk controls failed.

1.4 Identification of what went wrong and what risk controls need to be placed to avoid further risk management failure.


In order to examine the ineffective risk management practices that resulted in major failure, the paper will review a case study that reflects a major disaster that occurred due to the failure of risk management practices (See appendix 1). Drawing from the literature review of the case study, following issues will be addressed:

2.1 Application of theories to explain the ineffective behaviour of key individuals and groups.

2.2. Identification of actual leadership process / style and that which was really needed in this situation.

2.3 Explanation of what went wrong and what support is further needed to strengthen the organisation’s ability to cope with the risk.
2.1 Application of theories to explain the ineffective behaviour of key individuals and groups

In order to assess the ineffective risk management practices, the paper implies Control Objectives for Information and related Technology (COBIT) framework (IT Governance Institute 2007). This framework has been specifically chosen to make an assessment of management’s ineffective behaviour towards risk management due to its strength of integrating various business domains. Therefore, it has been learnt that implication of such a comprehensive framework can facilitate modern businesses that primarily requires functional integration so that each business function and process works towards common business goals. The framework divides business operations that should be mainly addressed by IT and Information Systems (IS) into four domains: a- plan and organise, b- acquisition and implementation, c- delivery and support and d- monitoring (ITGI and OGC 2005).

Plan and organise: This phase of the framework embraces the strategic intents and the tactics through which the IT can be business enabler towards the attainment of business objectives. Planning and organisation also identifies various perspectives of the way IT works as a business enabler and prepares the organisational infrastructure to further support the IT and business strategy. The main objectives of this domains are a- to ensure that the IT and business strategies stay aligned, b- organisational resources are optimised and used at the allocated places, c- all the members of the organisation keeps a complete understanding of the IT objectives, d- the associated risks with IT have been indentified and managed, and e- the quality of IT and business systems is appropriate for the business needs.

Acquire and implement: This domain works as the first step towards integrating IT strategy with the business strategy. IT solutions are identified, developed, acquired, implemented and integrated with the business processes. Any modifications and changes in the existing business systems are covered by this domain to ensure that IT objectives don’t conflict with the business objectives and strategies and new system doesn’t introduce any threats to the old systems. The objectives of this domain are to identify that whether or not: a- new projects deliver solutions that satisfactorily meet the business needs, b- new IT / IS projects are
delivered in time and doesn’t exceed the allocated budget, c- the new systems work with the old business systems and any confrontations aren’t observed and d- the changes incurred with the new system don’t disturb the previous business process and system.

Delivery and support: This domain delivers the required services and includes service delivery, security management and business continuity, service support for users, data management and operational facilities. The objectives of this domain are to ensure that a- IT services are delivered in alignment an accordance with the business priorities, b- IT costs are optimised, c- workforces have been appropriately trained to use the system, d- the confidentiality integrity and availability of the information security remains intact.

Monitor and evaluate: This domain covers the performance management, review, monitoring and evaluation of internal controls / countermeasure and regulatory requirement and compliance. The objectives of the domain are: a- IT performances are measured to detect the problems before they become disasters, b- management’s assurance to place effective and efficient internal controls, c- IT performance is linked to meet the business objectives and d- the confidentiality integrity and availability of the controls remain intact.

Forming these four domains as a basis for explaining the ineffective behaviour of key individuals and group i.e. board / executive, business management, IT management and audit / compliance committee called as ‘management’ by this paper, following findings have been gathered:

2.1.1 Due to management’s negligence of the first domain of the framework i.e. plan and organisation, following issues were triggered: a- non - alignment of IT and business / hospital strategy, b- scarcity of optimising the organisational resources, c- lack of user understanding of the objectives of the LASCAD system, d- ignoring / miscalculating risks associated with failure of LASCAD system and e- not evaluating the quality of the LASCAD system for its desired performance and delivery.

2.1.2 Implying the second domain i.e. acquire and implement to explain the management’s ineffective behaviour, following problems have been identified to be surfaced at the situation:
a- negligence in evaluating the competency and capability of the new system i.e. LASCAD system for delivering the solutions it has been designed for, b- ignoring the risk factor i.e. will the implementation of LASCAD system be effective and done in a desired manner?, and most importantly c- ignoring the prime question that will any changes made to LASCAD system will introduce new vulnerabilities in to the existing system? It has been assessed that while the existing system was being upgrade, the management perhaps ignored the fact of introducing new weaknesses and threats to the existing system.

2.1.3 The third domain of the COBIT framework is concerned with delivery and support of the new or upgraded system. An explanation of management’s unproductive behaviour through this domain yields that a- the IT / IS services were not being designed and delivered in line with hospital’s requirements and priorities, b- the cost of system development may have not be optimised or exceeded the allocated budget as a result of which its maintenance procedure was ignored, c- the workforce may not be competently and appropriately trained to use the LASCAD system efficiently and safely and d- the confidentiality, integrity and availability (CIA) triad may have been intentionally or unintentionally broken. Confidentiality means that the data / information remains private to authorised personnel only, integrity of data / information means that the data hasn’t been changed and availability means that the data / information is always available whenever needed. In the examined case, CIA triad has been assessed to be broken i.e. data / information wasn’t available when needed.

2.1.4 The fourth domain of the COBIT framework i.e. monitoring the information system, management has been assessed to be ignorant towards the following essential needs of the system: a- measuring the performance of the LASCAD system and its users in a periodic manner so that the problems can be identified before they transform into disasters and b- the need of an independent assurance that ensures that critical areas of the system are operating as they are intended or designed to.

2.2 Identification of actual leadership process / style and that which was really needed in this situation
To further evaluate and make recommendations for improvement, the paper now reviews different leadership styles and identifies the leadership style that was needed in the situation.

Lewin identifies three styles of leadership: a- autocratic, b- democratic, c- laissez- faire (Lewin; cited by Wetherell 1996). Autocratic leader make decisions without gaining consent of his team. This leadership style is effective when leader has to take quick decision, team members’ input / comments aren’t required and the leader can ensure that the outcomes of the decision doesn’t require team’s agreement. The second leadership style is democratic style that practices allowance of team input prior to making any decisions. Democratic leadership style is required when the outcome is affected by the team’s agreement however it may be difficult to manage too many inputs by different team members at one time. Lastly, laissez - faire style allows team to take most of their decisions as found appropriate by the leader. This leadership style is suitable when the team is highly competent, capable and motivated enough to make decisions that are in the best interest of the business. In addition to above Adair (2007) also articulates ‘transformational’ leadership style. This leadership style has been assessed to be falling under Lewin’s laissez – faire style. The traits of transformational leadership style suggested by Adair (2007) are: a- charismatic, b- inspirational, c- intellectual stimulation and d- considerate.

Referring back to the case study that articulates failure of LASCAD system which resulted in loss of lives of 20 -30 people, the paper suggests that the most suited leadership style in the given situation would have been transformational style. This recommendation has been made based on the traits of this leadership which fulfills the requirement of the incident that could have been avoided through effective risk management and leadership practices. Following points further explain the recommendations made for the chose leadership style:

2.2.1 This leadership style has been proven to effectively meet the challenges through reflecting business vision and mission through business practices. Eventually the leader is successful in gaining the respect and trust of his sub-ordinates and peers.

2.2.2 This style also inspires people so that the expected outcomes of performance delivery, needs and demands of the business, and the leader are effectively communicated.
2.2.3 The leader stimulates its people through his intellect so that knowledge, experience, organisational norms and beliefs are transferred on to his people. The idea here is to develop a knowledge organisation.

2.2.4 The leadership style reflects consideration as its prime element through providing face-to-face attention to individual members and providing coaching and mentoring. This action results in gaining people’s trust and confidence in their leader.

The situation that was faced was a result of various factors that failed in attaining the objectives i.e. performance of the information system (LASCAD) as expected. In addition to ineffective risk management, ineffective leadership style may also have been a possible cause. The following section will now evaluate what went wrong at the organisation and what leadership style and risk management practices could have avoided the situation.

2.3 Explanation of what went wrong and what support is further needed to strengthen the organisation’s ability to cope with the risk.

Drawing from the assessments made in the previous sections, the paper now makes an assessment of a- what actually went wrong and b- what could have been possible done to avoid such a situation again.

2.3.1 What went wrong?

A technical analysis of the system made by the same case study surfaced that the system didn’t face any technical failure however the actual failure of the system was not meeting the needs, demands and expectations of the stakeholders. Taking an account of the system failure in context of risk management, clearly there were ineffective risk management (risk analysis and assessment) initiatives taken. Risk analysis refers to identification and analysis of risks and its associated vulnerabilities. Risk assessment extends out to evaluating the existing countermeasures, their appropriateness and capability to manage the identified risks (Ahmed
2007). Therefore, ineffective risk management can result in exploiting the vulnerabilities associated with risk. Following factors have been identified that contributed towards ineffective risk management practices:

2.3.1.1 Lack of management’s commitment that resulted in ineffective management of risk. Due to lack of management commitment, communication about the importance of meeting the identified requirements and attaining targets were affected.

2.3.1.2 Lack of end user involvement in development of information systems which means that the developed system didn’t effectively serve its purpose.

2.3.1.3 Failure of management in gaining users’ / employees’ commitment resulted in comprehensively understanding the importance of the system and its delivery targets.

2.3.1.4 Lack of user / people awareness across the enterprise means that people aren’t aware of its importance, how to use the system, whom to report, whom to consult incase they need further guidance etc.

2.3.1.5 Insufficient user training and development means that people haven’t been satisfactorily trained to use the system effectively.

2.3.1.6 Disintegration of other information systems and LASCAD means that other functions and LASCAD may not be working together rather they may be conflicting with each other.

2.3.1.7 Lastly ineffective leadership style practices by the management means that the user involvement while development of the system had been absent. Even if the users were involved their opinion were never considered by the project leader. This refers to autocratic leadership style where team members’ opinions and comments aren’t valued based on an assumption that their opinions and comments aren’t required. Furthermore, the leader assumes all responsibilities, leaving team members feeling less valued and not empowered. This leadership style doesn’t delegate responsibilities where members feel mechanical and less creative. An autocratic leader is commanding and believes in task accomplishment rather than development of him as a leader and his sub–ordinates. This style of leadership is more suited with old fashioned organisational infrastructure with high bureaucracy. It is therefore suggested that in case of
failure of information systems, the project leader may have practiced autocratic leadership style, which eventually resulted in failure.

2.3.2 What could have been done better?

In context of the examined case study, the LASCAD system has vulnerability such as incapability of handling the volume of the calls that were received at the night of the incident. This vulnerability may have been ignored as a result of which the system faced a risk. This risk can be explained as incapability of handling expected volume of calls. The effective risk management practice hence would have been to:

2.3.2.1 Identification of the risk
2.3.2.2 Evaluation of the probability of risk occurrence
2.3.2.3 Evaluation of the impact (damage or disaster that will be caused to the hospitals, aligned institutions such as NHS and population relying on this system) of risk occurrence
2.3.2.4 Evaluation of the existing risk control measures
2.3.2.5 Making recommendations to control measures so as to mitigate or transfer the risk and
2.3.2.6 Establishment of a comprehensive system that monitors and evaluates the risk controls measures for their effective performance.

From the perspective of effective leadership style, following recommendations have been made inspired by Aidair (2007):

2.3.2.7 The project leader who is responsible of implementation and development of the LASCAD system should evaluate its leadership style through carrying out a survey regarding peoples’ views and opinions about his leadership style. It is however important that this survey is free of any influence and is conducted in a receptive and relaxed environment so that appropriate lessons can be learnt and improvements are made to avoid similar mistakes in the future.
2.3.2.8 There should also be an establishment of effective communication channels between the management and the team members so that the voice of the team
members are heard and valued as appropriate. It is imperative to note that the team members are the ultimate end users of the information system therefore it is possible that they know more than the leader about the specified situation.

2.3.2.9 Establishment of effective communication channels also means that leader is well-aware of his team’s opinion about the progress and development with the project i.e. development / up gradation of the LASCAD system.

2.3.2.10 The team leader should also acknowledge and reward the team members so that their good performance and behaviour is appreciated and consistent. This will also make the members feel valued, hence more productive and motivated than before.

2.3.2.11 The members should also be provided opportunities of job delegation as appropriate so that their motivational level and spirits are kept high at all times. This results in effective behaviours and productivity of the employees.

2.3.2.12 The leader should also lead by setting examples rather than just passing orders.

2.3.2.13 The performance levels of the people should also be consistently monitored and evaluated so that poor performances can be identified and differentiated from the good performance within appropriate time frame that allows room for improvement.
Appendix

Appendix 1: London Ambulance Service Computer Aided Despatch (LASCAD) system has been designed to work in the following process:

- The system receives an emergency call
- The details of the call are recorded
- The details of the incident are recorded
- Pinpoint incident coordinates with the system
- Incident location are displayed
- Dispatcher alerts the ambulance
- A message alert is being sent to the ambulance
- The system locates the nearest ambulances and determines the nearest ambulance

On the night of 26th October until the morning of 27th October, the HQ of LAS (ambulance service in the UK) received unusual number of calls i.e. approximately 600 calls more than the usual number of calls. Due to the system failure, many calls were wiped off the computer screen. This malfunctioning resulted in mass of automatic alerts generated that indicated that calls made to the ambulance hasn’t been acknowledged. The result of failure of information systems later claimed the loss of lives 20-30 people. A detailed assessment of the system failure showed the precise problem which was the inability of the system to cause response times to become...
intolerable. Conclusively the series of events that caused such problem can be seen as over burdening of the system that lost its capacity of handling the calls after the certain period of time of implementation.

References and bibliography


COSO (2004), Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, AICPA, Jersey City, NJ,


SENIOR SUPERVISORS GROUP (2008) ‘Observations on risk management practices during the recent market turbulence’, Senior supervisors group


WETHERELL, M (1996) Identities, groups and social issues, *Published in association with The Open University Volume 3 of Social psychology Social psychology : personal lives, social worlds ; D317*, SAGE


WILLIAMS, A et al. (1989) Risk management and insurance, Irwin, McGraw Hill
