It risk analysis case study

Information Technology is vital to every business today, since most businesses today are linked together with high speed broadband networks, high definition screens; superfast computers only make them a treat for a user.

So, if the IT fails the businesses suffer huge losses in a matter of minutes for e. g. the London stock exchange has an IT failure it could possibly mean a loss of thousands of pounds every fraction of a second. Every Risk no matter how big or small is a potential threat for e. .

a small cut on the hand could turn gangrenous over the period of time, what are we prescribed to do then, we would lose our limb, IT too is similar. A proper analysis and management is necessary to keep the IT in a good shape. Businesses understand IT as a risky proposition since they believe an IT system might last a while but would invariably die because of the stiff competition. Every time a new technology erupts on the market the one previous to it dies either a sudden or a slow death. For the past 4 decades IT has been a boon to the service industry making itself a slave science by supporting other sciences to grow, but very little effort has been made to log the number of times IT system failed and a even poorer job is done in logging the reasons that led to the failure. Most often the same mistakes are repeated but no serious lesson are learnt.

We believe it’s high time we start logging our failures because a shocking 60% of all IT projects fail even today. Normally, IT Risks are detected pretty late which leads to a failure it happens because a proper analysis and assessment is lacking. A good management would always like to know where

and how its investment will be used in and hence Risk Management is used to analyse and manage their risks in a more strategized format. 2.

0 Risks to the Organisation and its IS/IT Below is a list of risks that have been identified by us, each list is separated by category, in which each category will list different types of risks. Identification of risks; physical ? fire ? smoke/fumes ? explosion/impact ? temperature/humidity ? flood ? electricity Identification of risks; poor management ? poor communication ? unsuitable management ? accessibility denial of access Identification of risks; quality of software ? compatibility ? use of third party software Identification of risks; software. (active) ? virus ? worm ? logic bomb ? trojan horse ? spammer ? auto-rooter ? mobile code ? terrorist attack Identification of risks; Human interaction. ? loss of key staff ? terrorist attack ? usurpation. ? malicious action. Each list will fit into one of the following categories; ? disclosure ? modification ? destruction ? denied access Destruction Fire, smoke/fumes, explosion/impact, temperature/humidity, flood, virus, worm, logic bomb, trojan horse, terrorist attack.

Modification accessibility, virus, worm, logic bomb, trojan horse, auto-rooter. Disclosure accessibility, terrorist attack, malicious action, usurpation. Denied access loss of key staff, denial of access, malicious action, spammer Explanation of identified risks Fire The entrance to the building has a set of gas canisters, which are extremely hazardous. If these canisters were to erupt, then a fire would be the result of that. A fire could spread and cause an immense amount of damage to both equipment and to the building itself. IT systems are very unlikely to survive such a scenario.

Smoke/fumes Within the building there is an allocated spot for the machine and vehicle areas, both of which have 2 PC’s within them. A PC does not do well in an environment that will generate both heat and a fume, which is what will happen when you locate a computer near, or in the same room as a vehicle. The imprecation is long term damage to the components within the PC. You may find that the computer will slow down, and then eventually stop working. With a more suitable location, or with better protection against the environment, the PC’s could last a lot longer.

Explosion/impactThe gas canisters are again a problem. If they were to erupt it would cause an explosion, which would tear into the building. The impact would damage everything within a certain radius, depending on the intensity of the explosion itself. The damage caused would not be repairable, but would need to be replaced fully. Not only would an incident like this effect the building, but also the psychology of customers and employees that choose to visit the building.

Temperature/humidity Computers need the correct temperature and humidity to be able to function at its best performance. Computer also needs a steady environment for them to last as long as possible. If the temperature and humidity are too high, then a noticeable change in performance and life of all computers within the area where the temperature and humidity are high. Flood If a flood were to occur, then a shorting of electrical equipment would occur. With the shorting of the equipment, the equipment may become damaged. A flood would be detrimental to the building, causing damage to everything that is surrounds.

If water were to reach any IT equipment then the most likely outcome would be that the equipment would have to be replaced. Electricity All IT equipment needs a consistent supply of electricity to work. There is always going to be a risk of electricity cutting out, whether if is caused by power plants, or by those within the building, or by any of the other risks outlined above. A sudden lack of electricity could damage computer components, and a lack of electricity over a period of time will be detrimental to the company. Poor management Poor management covers a lot of things, poor management of systems, and poor management of staff.

The effects of poor management within the company can affect the flow of work, and with poor management comes poor relationships, which can eventually become risky. Management on systems has to be top notch to ensure that nobody who shouldn’t have access, don’t have access to important system files. Management has to be clean and stable to make sure that the Staff sticks to their responsibilities. Accessibility Two main risks with accessibility, one being lack of access, and the other being unauthorised access. At all times, those who are supposed to have access to certain files, must have access to those files. If administration staff is not able to gain access to their own systems, then you have problem.

Unauthorised access can occur in multiple ways, and can affect the company in different ways, which range from disclosure of information, to corruption of data. Good relationships have to be maintained with current staff, and unauthorised access has to be prevented before the attack can cause any damage. Compatibility/third party software Within companies, it is best to use software that is of the same make, instead of using different types of

software on different PC’s. This is to ensure that each PC is using files that are compatible on each other PC. In the event of a loss of systems, it is within the interest of the company to be able to use other PC’s as a temporary set-up, instead of having to halt the work process all together.

The risk of using the most well known types of software is that there are people who will find the vulnerabilities within them, and exploit. But you have the idea that the staff may not understand or be familiar with third party software, so software that is common should be kept up to date at all times. Malicious softwareThis includes viruses, worms, logic bombs, Trojan horse, and spammer. These types of software can enter onto your system in various different ways. Through email, storage media are perhaps the most common.

This type of software can affect your system in various ways, typically they are created to do more harm to the flow of system work than to actually gain anything from the attack, which makes them easier to detect since the “ attacker” doesn’t want any specific information from the system. Usurpation Any member of the company who has access to a computer could potentially misuse it. This is a way in which outside intruders can gain access to inside system information. Malicious software may enter the company through any member of the staff. Loss of key staff The company has the following members of staff: ? Managing Director ? 2x Design Engineers ? 3x Mechanical Engineers ? 1x Electronic s Engineer ? 1x IT Support Engineer ? 2x Administrators In bold are the most worrying loss of members, if such a scenario were to occur. Losing one engineer designer would cause

disruption, but there would still be one designer left with knowledge of the current design process.

The company has only 1 electronics engineer and 1 IT support engineer. They could be replaced, but losing either of them suddenly could cause problems with negligence of IT equipment. Malicious action Administration has the most power when it comes to the company network and access to it. It is for this reason that they also have the easiest chance of doing damage to the network and/or systems. It would be a lot easier for a member of staff with admin privileges to do damage, a virus, time bomb, key logger; etc could be uploaded to the system and could lay in wait for a specific time to activate. Any member who has access to a computer could potentially misuse it.

This is also a way in which outside intruders could gain access to inside information, through the staff misusing the computers. Any member of the company who has access to a computer could potentially misuse it. This is a way in which outside intruders can gain access to inside system information. The misuse of computers Malicious software may enter the company through any member of the staff.

Actions must be taken to prevent this happening. 3. 0 Evaluation of Risks associated with Threats MalwaresMalwares aka malicious software’s are the major threat to an organisation on the internet. “ These malwares are categories into many forms such as: Computer viruses, computer worms, Trojan horses, Logic bombs, Spywares, Adware, Spam and Popup” (TechFaq, 2009). It is high risk aspect for the FC racings as these could affect their

computers to turn into terribly slow and also, it can take control of any browser and can track their browsing history (Baratz, 2009). These can also slow down the performance of the computers which affects in restarting on the computers.

FC racing can loose important data if their computer system automatically restarts. Security provisions Defective doors and alarms are examples of security provisions which could have an effect on the demolition of asserts and amenities. The loss of these, would affect the IT system of the company as well as slowing down the production of products. If thugs and thieves find the important information of the company, i. e. customer details and confidential information which are related to workers, they could transfer that information to the rival companies.

Electronic failurePower cuts, web server failure, hardware failure and PC system failure are all consequences of electronic failure, which can result in a complete failure of IT and communication within the entire organisation. An entire crash of IT would result in a disaster as all the data will be completely vanished and therefore, IT facilities would be out-of-the-way leading to productivity enclosed by the organisation being slowed down until it is improved. Power cuts can lead to a server not working which effects in loss of information leading to economic difficulties within the organisation. Server failure would cause a heavy disaster to the company which could result in loss of important information. Company could loose important information if the hard disk breakdown would come about. If a PC system fails it will guide to an entire loss of vital computing services follow-on in loss of communication within the administration.

Health and safety (Medium risk factor) It is the organisations responsibilities to insure that their employees fell safe and secure within the workplace, which may include factors such as; natural disasters or accidents at work. An organisation should provide safe and healthy working environment for its workers. Employees should be given the correct education and training about health and safety. In case of emergencies there should be an assembly point for everyone to gather safety regulations. And in case of emergencies, premises should have several emergency exits with green lights on them to guide every one out to a safe place. Premises should also have sirens for warnings.

If possible organisations should carry out regular practice drill tests in the premises o make sure everyone is properly trained and all exits and sirens are properly working. Health and safety is a major issue in all work places. Our given organisation does not follow any of these features at all. We know this as there are no signs of any fire exists in the premises and there are no marked assembly points for everyone to gather for safety reasons. Moreover the entrance is surrounded with explosive gas tanks. This can lead to a big disaster.

For example if a gas tank explodes, it is dangerous for the organisation in many ways. Including having to close down the organisation for a week or more and can result in the organisation struggling to continue with business. Software and Application change (medium risk factor) There are some risks which can occur during the process of updating or changing software or an application, for their enhanced performance and better security. But there is

possibility that an updated version of a particular software or application may not work properly as previous ones.

Sometimes old files become incompatible with new a version of software or application, resulting in delay of particular tasks. If anything like this happens it can take from four to eight hours, resulting in precious time loss and paralysing the whole system. Consequently, the organisation can loose its valuable customers. Or there could be other ways, for instance; organisations may have got a new version of software or applications and try to send information to their customers but, the customer is unable to look at that information because they have not got the same version of software or application. This could result in disaster, in the sense that customers might get frustrated and decide to stop any further business with the organisation. ttps://www-304.

ibm. com/businesscenter/cpe/download0/160577/12_13. pdf The inability to operate (High risk factor) The loss of certain facilities can lead to closure of businesses. These can be a result from the loss of IT facilities, networks, and hard disks, updated versions of software and explosion of gas tanks.

IT facilities are responsible for printing, sending e-mails, audio equipments, video equipments, telephone system and all the soft ware available on operating system. If an organisation looses its IT facility, all it’s factors supported by them resulting in delay of services and it can take up to two to twelve hours to identify and fix that problem. Network failure is total disaster for an organisation as it includes the entire business working through the internet. Loss of network could result in loosing valuable customers and it

can take more than one day to fix this problem. Hard Disk failure means losing all the information about customers and products from that particular computer system, which can result in temporary denial of a few services. It can also take a day to change the hard disk and upload all the information on to it.

If any of the above mentioned, keep happening in a short interval of time it could result in reducing revenue or can even lead to closure of the organisation and bankruptcy. Data Classification (authentication) When being dependent on the internet for all its sales and trades of products all the applications on the web server should be identified and classifies the associated data. Classification of data shows who has access rights to the available resources, which is usually only to a few members of employees. It is vital that those who should have authority to allocate access rights and access level know who they are. This means if anything goes wrong in the organisation, related to data security, the authorised person has to report to the organisation.

If the organisation fails to take all these measures, it can lead to them loosing information or data from the organisation, which means the organisation, can not connect to their customers and can loose them. http://www. kpmg. ca/en/services/advisory/forensic/documents/FRM.

pdf http://docs. google. com/viewer? = v&q= cache: hWoh554Y4cEJ: wenntownsend. co. uk/pdf/Fraud_win08. pdf+what+are+frauds+within+the+organisation&hl= en&gl= u k&sig= AHIEtbTLJLPrEOI1I5QlYRePRfvM1NE4wA Fraud (Low risk factor) (9) Fraud

inside the organisation is stealing of important information such as the purchaser or buyer lists.

This could only happen if some disturbed worker within the organisation tries to steal it. This type of activity would have a harmful effect on the company which would affect its status, economic aspects and could cause in business shutting down. (GoogleDocs, 2008) ttp://cerncourier. com/cws/article/cnl/31988 Security risks http://www. theregister. co.

uk/2009/02/25/security_threats/ 4. 0 Countermeasures (RISK ANALYSIS TECHNIQUES) http://www. drj. com/new2dr/w3_030. htm Introduction: Risk means a chance or hazard for commercial loss but even then it is considered that a risk is an integral part of any business venture, we need to manage the risks and assess them at the start of any project a calculated risk has a brighter chance of turning out a fortune than a risk taken without a thought, risks could turn out fatal sometimes. Businesses have only recently started believing that Information Technology plays an important role in prospering them and if their IT fails their businesses would suffer FS Racing is no different.

IT has often proven to be high risk to businesses, with an ever changing facet that IT comes with. There is always a chance a new ICT might become obsolete in a few months of installation, but that is a risk that an enterprise has to take in order to give its customers and employees a better service. The use of the word ‘ risk’ is pretty confusing most times because it’s normally used in a phrase aying this is ‘ a low risk’ or vice versa I believe every risk is a potential threat to an enterprise. IT risks wouldn’t really go

away until a proper planning and tuning of IT is in place and businesses finally start believing information as the biggest asset to their enterprise. As discussed earlier there could be both direct and indirect consequences of an IT failure to FS Racing.

We must understand that each member of the team is equally accountable to the well being of the company and its information resources. Every risk is predicable said that a predictable risk could be a critical member of the team leaving or a fire or even a piece of hardware breaking down although they are all difficult to predict but predictable. Counter measuring those risks is the key to success. Indentifying the right user: Every user should be holding a valid password when using a computer.

It is always advisable that we use a combination of numbers, alphabet and special symbols in order to make it difficult to crack by unauthorized individual. Access Control: It means preventing users to view and access only a resource that they are entitled to view. It is often considered the next level of system security after identification of users. FS racing requires a role based access control to be in place. Encrypting data: Data encryption is a key policy for an enterprise as information plays a very important role in businesses today. The same applies to FS Racing as well since they might send design details to the racing teams they give support to.

Regular Backups and data archiving: Regular backups are necessary in order to keep the risk of data loss to the minimum archiving help us record and maintain the latest changes to the database. By archiving we can restore the database with minimum loss of data in case of a system failure. External

storage: External storage could be anything from a CD to a USB flash drive. To avoid data leakage we shouldn’t allow our employees to get these items in the premises. Countering Physical Threats: 1.

Fire: Fire is a major threat to FS Racing since they manufacture automobile parts which require soldering of parts, melting metals at a certain temperature for casting, etc. Fire can be counter measured by installing fire extinguishers, fire blankets, water and sand. . Flood/water leakage: Water logging can disrupt FS Racing’s everyday working since the new premises is a single storey building. Water logging can be counter measured by keeping all the important documents, ICT equipments, designs, machinery at a height. 3.

Explosion: By looking at the entrance of the enterprise we can be sure of explosion being a potential threat to FS Racing with the highly inflammable gas cylinders kept unprotected outside. Countering Non Physical Threats: They are divided as Threats and attacks. A threat might be data leaks, data corruption, etc whereas attacks might be active or passive caused by either an insider or an outsider. Malicious software: They are also popularly known as malware, these are a set of bad computer programs written specifically to disrupt the regular work. These programs have a tendency to self replicate and they also propagate themselves.

These malware have various terminologies like virus, Trojan horse, worm, etc. We can counter this malicious software by installing a Firewalls, Anti-Virus software’s and Anti-Spyware scanners. 1. Firewalls: Since internet plays

a huge part in FS Racing’s everyday business it is a necessity to install a firewall.

A firewall hence is a barrier between user computer and the internet. A firewall is used to avoid any unnecessary data to flow between the internet and the computer. They are further divided into hardware and software firewalls 2. Anti-Virus It is software which identifies and prevent computer from harmful software’s, for instance viruses etc.

Company can avoid being harmed by any virus or worms, if they follow simple steps such as: •Every Computer should have Anti-virus software and it should be updated regularly. Operating system should have the latest updates from its vendor, means it should to up to date. •Also, use of good and updated anti-spyware software •http://support. microsoft.

com/kb/129972 3. Spyware Scanners This Scanner is a must installed application in every computer because its main purpose is to scan for Spywares. Spyware automatically moves to computers when someone tries opening a website which has contaminated cookies saved on its server. The Spyware scanner automatically alerts the user whether to save the cookie from that website or not. http://www. tech-faq.

com/protect-computer. html Electronic failures: Power cuts could be fatal if not predicted and a backup plan is in place. Countering power cuts would mean FS Racing acquiring a battery run generator to provide essential services to the enterprise. These generators charge themselves when plugged into electrical sockets. Web Server failure could be a huge loss to the enterprise if not dealt in a professional manner normally, web servers are

the biggest threat to any business today since there are malware and hackers all over the web, it so becomes a priority to keep a check on it and detect any ill doing before the usiness comes crashing down.

The operating system and anti malware software needs to be properly installed and upgraded to avoid hackers getting attacking our computers. System and hardware failures causes work delays since most of the work is done using computers. To overcome it we need to properly and regularly check our hardware resources before initialising a new project. A mirrored backup of the designs is also required so that the data loss is at a minimum in case a hard drive fails. Health and safetyHealth and safety of employees is a major priority of any business. A health scare could be a person catching a cold to a person losing a limb at work.

To counter this threat an enterprise must ensure every employee is medically fit before joining and a regular health check up should be made compulsory, FS Racing should also merge with an insurance company and provide its employees with a customised insurance plan and part of their salaries should go to the insurance firms as a premium of their cover. Software application changeSoftware application change must be done with keeping an eye on the hardware and the existing software for compatibility since a major roadblock is inevitable if software and hardware aren’t compatible. To counter this problem we should firstly test any new software or hardware before implementing it in the current system. Fraud Fraud is also a risk by a disgruntled employee might try to steal some important information and hence any employee leaving the company should be barred

from using any IT equipments. Their company email should be closed as they quit.

Computers of employees should be monitored closely and regularly to avoid any wrong doings by them. 5. 0 Recommendation of measures to be taken to protect the business and priorities As the given scenario have so many draw backs and is not safe place to work. Firstly premises don’t have any entrance signs, which is a bad effect on the customers and also bad for business.

To improve this, an entrance sign is needed to be placed in the reception area. There are also no fire exits in case of an emergency. This can have an effect on the employees as it is a hazard and can lead to loss of life if a fire occurs. fire exits should be shown on specific places in premises and those are shown above.

As there is threat to computers and laptops in the Machine areas, Development and testing workshop and vehicle workshop, there are computer which can be damaged due to heat produced in all those areas can lead to disaster n delay in process and services. To over come this, we have come up with some changes in all those areas. Although the organisation have to spend some money on that but still it’s important and can protect valuable computers. Organisation have to build up a small cabin all those areas fitted with proper air conditioning, to protect computers from being damaged from heat produces in all those areas. These can be at following place in following rooms as shown in image above.