I.t faliure and dependence 1643

In Today" s Society we are so Dependent on I. T that the Consequences of its Failure May be Catastrophic. Discuss the Threats and Causes of Failure, and Steps Taken to Minimise it.

In today" s world it is impossible to run a large organisation without the aid of computers. Businesses hold massive amounts of important data, hospitals hold large amounts of confidential patient information and large scientific research projects hold important codes, formulae, and equations. The bottom line is that loss or corruption of this information is sure to result in bankruptcy, a substantial loss of customers, and even world-wide financial meltdown.

A dependency on technology is impossible to avoid aˆ“ even with its fatal consequences. Companies face the worry of information lost through hacking, virus corruption, and even physical threats such as fire and flood. Viruses are the most common threat to companies they can corrupt large amounts of files and data both kinds of virus, biological and electronic, take over the host cell/program and clone their carrier genetic codes by instructing the hosts to make replicas of the viruses. Neither kind of virus, however, can replicate themselves independently; they are pieces of code that attach themselves to other cells/programs,

Just as biological viruses need a host cell, computer viruses require a host program to activate them. Once such example of the damage done by viruses occurred in 1988. A Cornell University hacker named Robert Morris used the national network system Internet, which include the Pentagon's ARPAnet data exchange network. The nation's high-tech ideologues and spin doctors have been locked in debate since, trying to make ethical and economic sense of the event. The virus rapidly infected an estimated six thousand computers around the USA This created a scare that crowned an open season of viral hysteria in the media, in the course of which, according to the Computer Virus Industry Association in Santa Clara, the number of known viruses jumped from seven to thirty during 1988, and from three thousand infections in the first two months of that year to thirty thousand in the last two months. While it caused little in the way of data damage (some richly inflated initial estimates reckoned up to $100m in down time), the ramifications of the Internet virus have helped to generate a moral panic that has all but transformed everyday " computer culture."

Other worrying viruses include " Pathogen" which was created by Christopher Pile. This fatal virus wiped data from a computers hard drive, in 1995 he was convicted under the Computer misuse attack. Stephen Fleming a BT employee gained access to a database that contained hundreds of top secret phone numbers and addresses of government installations. Police managed to catch him, and he was threatened to prosecution under the first category of the computer misuse act. Meanwhile BT tightened their security.

One major bug that threatened to destroy all of our data was the Millennium bug. It pursued the media for months; it was difficult not to have heard of it. The problem was that many electrical items aˆ“ not just computers held a chip that kept track of the date, it was feared that after 1999 the date would switch to 0000 or 1900 and stop working all together. Millions of pounds were spent trying to outsmart the bug; no computers were sold in the years running up to 2000 without being " millennium compliant". Fortunately the bug did not strike, and now many anti-virus companies are being accused of conning industries into buying new software to tackle a non-existent bug.

Anti-virus packages are now one of the best selling types of software. Many companies offer bigger and better packages each year. " Norton" anti-virus software is one of the best selling packages along with " Dr Solomon" s" anti-virus toolkits. It is very sensible for every computer owner to have an anti-virus package. And it is vital for any company to have an advanced anti-virus package.

Data is also secured using a backup system. When processing information banks and businesses produce huge amounts of backup. Looking at the amount of backup created you may think that it is absurd. But for the business it secures information, any master data that is lost can just be brought up from backup files.

The problem is that backup files need room to be stored, and protection. Fire and flood produce an increasing threat to large backup files. To avoid these problems most companies store there backup files in a different building to their master files. This means that damage to one building forces the company to recall their backup files from the other building which will not have sustained damage (unless the company has very bad luck!)

Companies taking these precautions spend a huge amount of money on them. Updating anti-virus software, changing passwords and changing the location of tons of information can prove severely expensive. That is not to say that the companies are foolish, for the amount spent on prevention is only a fraction of that which would be forfeited from loss.

It is rather scary to think that we risk so much money and even lives over the loss of simple data. Space travel, vital medical care, stock markets, air traffic control, and transport all rely heavily on I. T to keep them going. It is fearful to think of the price we might pay if the I. T that we count on, failed.