## People and IT

Ever since industrial revolution, people have feared that machinery will replace workers, and Information Technology us no exception.

In spite of dire predictions, however, there is no evidence that the introduction of computers has led to mass unemployment – in fact, over computers have created all more jobs than have been replaced by them. Nevertheless, in some areas computers have substantially replaced the workforce. In the 1980s, thousands of factory workers were made redundant by the introduction of robots on the factory floor making everything from biscuits to cars. In the 1990s, thousands of clerical and white-collar workers saw their Jobs disappear with the introduction of company databases, desktop publishing, computerised accounting systems and increased automation in banks, building societies and organisations of all kinds, large and small.

Teleworking involves carrying out work away from the office and communicating with the employer through the use of a computer and telecommunications equipment. Often Tele-workers are based at home, but they can also work from Telecentres, satellite offices or even on the move. Although a study done in 1995 at Newcastle University found that less than 1 worker out off 100 was a Teleworker (spending at least half of their working week at home using the computer), organisation are becoming increasingly interested in various forms of Teleworking, which are becoming increasingly interested in various forms of Teleworking, which has benefits both for the employer and the employee. According to research done by Henley Business School in 1997, there are already 4 million Teleworkers in the UK.

Recently, the relative demand for skilled labour has increased dramatically. We investigate one of the causes, skill-based technical change. Advances in the Information Technology (IT) are among the most powerful forces bearing on the economy. Employers who use IT often make complementary innovations in their organi sations and in the services they offer. Our hypothesis is that these Co-inventions by IT users change the mix of skills that employers demand. Specially, we test the hypothesis that it is a cluster of complementary changes involving IT,

workplace organisation and services that is they skilled-based technical change. We examine new firm-level data linking several indicators of IT use, workplace organisation, and the demand for skilled labour. In both a short run factor demand framework and a production function framework, we find evidence for complementary. It use complementary to a new workplace organisation which includes broader job responsibilities for lineworkers, more decentralised decision-making, and more self-managing teams. In turn, both IT and that new organisation are complements with worker skill, measured in a variety of ways. Further, the managers in our survey believe that IT increases skill requirements and autonomy among workers in their firms. Taken together, the results highlight the roles of both IT and IT enabled organisational change as important components of the skill-based technical change.

Training staff in the use of new technology is crucial to the success of any computer system. Unless staff at all levels of an organisation know how to use the new technology effectively, investment in a computer system can be a waist of money.

When a new software package is introduced into a company, users at different levels of the company may require different levels of training. At the lowest level, for example, a clerical worker may need to know how to load a spreadsheet package, enter the daily or weekly sales figures and print a report. A member of the sales staff in electrical retailers may need to know how to enter customer's details to check their credit rating and reports, and how to use function keys to activate macros. These activities are taskbased.

A middle manager or knowledge worker on the other hand, may need skill-based rather than taskbased knowledge. A marketing manager who has to give a presentation on the expected sales of a new product may need to use a spread sheet to analyse and graph actual and projected figures and insert the results into a word processed report for the managing director. An office supervisor may design a style for all-international memos and reports, and create a template and macros to automate certain functions, using a word processing package.

It is continuing to take over more and more jobs in the workplace, this will lead to an eventual high job loss, so unemployment will be high.

Another fear point that some people fear is that in the future, we will make AI robots and they will overcome us, and then control us because they would be stronger and more intelligent, but this is a bit far fetched. A reliance on technology brings with it unavoidable dangers. Faulty hospital equipment that delivers the wrong dose of radiation, by -by-wire aircraft that develops hardware or software faults and fall out of the sky, software bugs that corrupt data held in massive databases, are just some of the catastrophes that can result from our dependence on technological wonders.

Ergonomics refers to the design and functionality of an environment, and encompasses the entire range of environmental factors. Employers must give consideration to :-

- **Lighting**. The office should be well lit. Computers should neither face windows or back into a window so those users have to sit with the sun in their eyes. Adjustable blinds onto a window should be provided.
- **Furniture.** Chairs should be adjustable height, with a backrest, which tilts to support the user at work and at rest, and should swivel on a five-point base. It should be at the correct height relative to a keyboard on the desk.
- Work space. The combination of chair, desk and computer accessories (such as document holders, mouse ad mouse mats, paper trays and so on), lighting, heating and ventilation all contribute to the workers over all well being.
- **Noise.** Noisy printers, for example, should be given covers to reduce the noise or position in a different room.
- **Hardware.** The screen must tilt and swivel and be flicker-free, the keyboard must be separately attached.
- **Software.** Software is often overlooked in the quest ergonomic perfection. The EEC directive made a clear statement about the characteristics of acceptable software, requiring employers to analyse the tasks, which their employers perform and to provide software which makes the tasks easier. IT is also expected to be easy to use and an adaptable to the users experience.

Computers can be responsible for a whole raft of health problems, from eyestrain to wrist injuries, back problems to fetal abnormalities, stomach ulcers to mental collapse. Articles appear regularly in the newspaper

relating stories of employers who are suing their employers for computer related illnesses.

Not so long ago it was thought that the widespread use of these fantastic machines, that could perform calculations and process data with lightning speed and complete accuracy would free up humans to work maybe only or three hours a day, while the computer did all the loins share. In fact, people seem to be working harder than ever, trying to keep up with the output of their computers. Human beings are the weak link in the chain, needing food, rest, a social life; they are prone to headaches, stress, tired limbs and mistakes

New technologies generally create new opportunities for crime, as soon as one avenue is blocked to the criminal, another one is discovered. As information technology has spread, so too has computer crime and abuse. The Internet for example is not only used for hackers and terrorists. Their activities include planting computer viruses, software bootlegging, storing pornographic images and perpetrating all sorts of criminal activities from credit card fraud to the most complex multinational money laundering schemes. Computer abuse refers to acts that are legal but unethical.

Hacking is defined as unauthorised access to data held on a computer system. The extent of hacking is extremely difficult to establish as it is usually only discovered by accident, with only about two percent of security breaches discovered a result of positive action on the part of security staff.

Data can be stolen by illegally accessing, or by stealing the computer on which the data is stored in. In December 1990 Wing Commander Farquhar notebook computer was stolen from his car when he left it unattended for a few minutes. It contained the preliminary allied invasion plan for the impending Gulf war, and could have had potentially disastrous consequences.

The rapid progress of computer technology has led to the need for new laws to be introduced so that all perpetrators of computer crime can be prosecuted. Laws in the US impact on computer users in this country, since the majority of systems and Internet content is American. A general approach to a commission and Internet -Related laws throughout the European Union formed part of a proposed European commission directive discussed by member stated on October 1996.

In early 1980s in the UK, hacking was not illegal. Some universities stipulated that hacking, especially where damage was done to data files, was a disciplinary offence, but there was no legislative frame work within which a criminal prosecution could be brought. This situation was specific criminal offences to deal with the problems of hacking, viruses and other nuisances.

- Unauthorised access to computer programs or data
- Unauthorised access with further criminal intent
- Unauthorised modification of computer material.

Computer software is now covered by the Copyright Designs and Patents Act of 188, which cover a wide range of intellectual property such as music, literature and software. Provisions of the Act make it illegal to:-

- Copy software
- Run pirated software
- Transmit software over a telecommunications line, thereby cheating a copy.

Software can easily be copied and bootlegged. In addition, the programming ideas and methods can be stolen by a competitor; A pple programmer to revere engineer machine code to establish the specific algorithms used, so that they can be copied sued Microsoft maybe years ago. Some software manufacturers put fingerprints into the code – little oddities, which do not effect the way the programme runs – so if the same code is found in a competitors program, they can prove that it was illegally copied.

The Business Software Alliance in 1998 targeted some 20,000 small and medium-sized companies to ensure that all software being used is correctly licensed. Offences include using pirate copies of software and using software on more machines that are permitted under the terms of the licence.

A few ways in which a compute user could protect the computer from hackers and viruses are: -

- Having a fire wall on the computer to stop hackers from invading the computer
- Have the password for the computer changed regularly, this is because it will stop people from guessing the password easily

• Have an anti-virus program on the computer, this detects and cleans the computer from most viruses as long as it is up to data.

The rights to privacy are a fundamental human right and one that we will take for granted. Most of us for instance, would not want our medical records freely circulated, and many people are sensitive about revealing their age, religious beliefs, family circumstances or academic qualifications. In the UK even the use of a name and address files or mail shots are often felt to be an invasion of privacy.

With the advent of large computerised databases it became quite feasible for sensitive personal information to be stored without the individual and accessed by, say, a prospective employer, credit card company or insurance company to assess some bodies suitability for employment, credit or insurance.

Below is the data protection Act that must be followed by all companies.

- Fairly and Lawfully processed
- Processed for a limited purpose
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Not transferred to countries without adequate protection.