lobbied for some time for private keys to be independently stored, so that encrypted communications could be monitored when national security is considered to be at risk.

9.8 Exercises

9.8.1 B2C e-commerce

What advantages does the customer stand to gain from B2C e-commerce, compared with traditional business models?

Can you think of any potential disadvantages?

9.8.2 C2C e-commerce

Give reasons why internet auctions are a common source of fraud, and suggest control structures that could be put in place to reduce this problem.

9.8.3 B2B e-commerce

Explain how B2B ecommerce could contribute to each of the alternative strategies for competitive advantage (low-cost, differentiation, niche marketing) that were described in the previous chapter.

10. Security and Social Issues

We all know why computers are taking over from human processors. They are much cheaper in terms of their cost/performance, can handle large volumes of transactions at great speed, do not make mistakes, are not members of workers' unions and do not take holidays or sick leave. In the early 1980's the computer was still an object of some mystery, hidden in large buildings and operated by specialist personnel. Today the computer is everywhere: in every office and many homes; and individuals with limited or no computer expertise are becoming a minority.

However, computers also offer new opportunities for fraudulent and illegal activities. Well publicised computer crimes of the last decade have included:

- **The Equity Funding Disaster**. The top management of Equity Funding created billions of dollars of bogus insurance policies and sold them on to re-insurers. The motivation was to survive a serious cash flow problem and the intention was to buy back the policies and hide the fraud when the business began making money again. Unfortunately the problem persisted and the fraud grew to such proportions that the company actuary calculated that soon they would have insured more phony people than the entire population of the United States.

- **Mamalodi Sundowns vs Standard Bank**. The owner of a South African football team required funds to purchase players and support an extravagant life style. His girl friend was working in the head office of a large bank and was responsible for allocating inter-branch transfers of funds from one account to another. Over a three year period she transferred over R10 million into accounts controlled by her friend and covered the fraud by moving new funds into the accounts previously stripped. Like most frauds of this type, they can remain undetected for many years until the staff member is not available to continue the manipulation. The individual went on holiday for a week and her replacement noted some irregularities and called in the auditors to investigate.

- **The Rifkin Caper**. A computer contractor to a Californian bank used his inside knowledge to find the necessary passwords to authorise electronic transfers of money, and made a $12 million transfer from a client's account to a Swiss bank account under his control. He then travelled to Switzerland and purchased diamonds with the funds. Back in the USA he was apprehended in a police trap while trying to sell the diamonds. Of interest is the fact that the client only discovered the loss of the original funds when police enquiries concerning the diamonds began. The contractor's name was Rifkin and he almost escaped going to prison because of technical irregularities in police arresting procedures. He has since served his time in jail and is now a computer security consultant.

Because much of the data processing that takes place in an information system is not visible to the naked eye, controls must be built in to ensure that business transactions are correctly recorded and processed. This chapter also looks at some of the threats faced by computer systems, and discusses how the computer has changed our daily lives, both at work and in the home.

Some of the issues that are addressed in this chapter include

- security within the organisation: fraud and access control
- security beyond the organisation: hackers and viruses
- computers and unemployment
- operational problems and errors
- computer monitoring and invasion of privacy

10.1 Security Within the Organisation

Security risks within an organisation include the processing of fraudulent transactions, unauthorised access to data and program files, and the physical theft or damage of equipment.

10.1.1 Fraud

Computer fraud is increasing at an alarming rate. **Fraud** can be defined as the manipulation of the records of an organisation to conceal an illegal act (normally the theft of funds or other assets). Computers can make it easy for employees in particular to defraud the organisation, in particular when the level of security and internal control is lax. In manual systems, a common control to limit fraud is to involve two or more people in a process, each one effectively controlling the activities of the others. We call this control process separation of duties. For example in a payroll system one might give an individual the authority to approve increases, another the task of updating the computer and the third the responsibility to distribute funds to employees. Without collusion between them, it would be difficult for any one of these individuals to steal funds from the payroll system and hide his tracks. Unfortunately, in many computer systems, too many separate functions have been computerised and often there is a single clerk responsible for running the entire payroll process. In these situations, anyone who has access to the application can take the opportunity to commit fraud. The most common fraud tactics are:

- **Entering fictitious transactions**. Most frauds are committed by employees using the system in the normal way to enter fictitious transactions. No special technical knowledge is required and the employee relies on the fact that management supervision of the process in weak.
- **Modification of computer files**. Normally requires a little more technical expertise as this would involve, for example, the increase or reduction of amounts held on the master file, which cannot be changed within the application without an appropriate transaction (such as a payment).
- **Unauthorised changes to programs**. This type of fraud is usually limited to staff with programming expertise. A common example is the s**kimming or salami technique**. In a payroll system this would entail deducting a small amount from each individual salary cheque and adding the total to a select individual's payment. The secret behind this technique is that employees are unlikely to notice a change in their salary (PAYE and other deductions often cause regular variation in the total) and the total payroll will balance (the total amount being paid is the same.)

How does an organisation limit fraud? Experts suggest a three-pronged attack. Firstly the organisation must stress the need for honesty and ethical behaviour in all business activities. Managers must lead by example, new employees must be screened and staff training must support this theme. The second concern is the level of opportunity in the organisation to commit fraud. There must be strong internal controls, separation of duties, restricted access to sensitive applications and constant management supervision. Audit trails are used to record the origin of every transaction, and sequential numbering ensures that records cannot be deleted or reports destroyed. Finally, where a case of fraud is discovered, action must be taken against the offender. Many organisations prefer not to prosecute employees suspected of fraudulent behaviour because of the negative publicity they will receive in the press. This in itself encourages criminals to repeat the activity in their new working environment knowing the likelihood of punishment is remote.

10.1.2 Unauthorised Data Access

Password protection is the most common method of protecting corporate data. Nevertheless, fraudulent transactions are often carried out by unauthorised users who manage to gain access to the corporate network by using the login details of another user. One way of achieving this is through a **terminal spoof** - a simple yet effective approach to finding other user's passwords. A terminal spoof is a program that runs on a machine and looks like the normal login screen. Once a user has given his or her user-id and password, the terminal spoof will record both on the local disk or server, give what looks like an authentic error message (such as invalid password – please re-enter) and then passes control to the real login program. The criminal will pick up the passwords later to gain access to the system masquerading as the unfortunate victim.

Other criminals simply make use of an unattended computer that has been left on by a user who has logged in to the network and then left the office. Time-out or screen-saver programs with password protection provide a simple barrier to this approach. In addition, locked doors are a traditional means of excluding undesirable visitors.

Other dangers of which managers should be aware include the **Trojan horse**, in which **c**ode is added to a program, which will activate under certain conditions. For example, a computer consultant in Johannesburg had a client in Durban. He placed a Trojan horse in the payroll program so that it would malfunction while processing the June payroll. They would fly him down, all expenses paid, to fix the problem and stay for the Durban July horse race. Once this had happened for the third time, another consultant was used who uncovered the offending code.

Another risk is the **Back-door technique**. When programmers are building systems, they may try to bypass all the access security procedures to speed up the development time. In some cases, these "back doors" have not been removed and the programmer can gain illegal entry into the production system.

10.1.3 Sabotage and Theft

When computers were the size of small houses and hidden in secure computer installations, then theft of computer hardware was rare. Today, PCs are on most desks and in many cases

they have to be physically bolted to the table to prevent their disappearance. One famous case of theft involved a laptop computer stolen from the back seat of a car in the USA in early 1991. On the hard disk was the master plan for Desert Storm, the details of how the United States and her allies would attack Iraq.

Mobile computing devices are especially vulnerable to theft, and limiting of physical access to equipment is the most effective first line of defence. Restrictions to entry can be based on electronic locks, activated by means of magnetic disks or swipe cards, or on advanced **biometric** devices that identify the individual based on characteristics such as fingerprints or the pattern of the retina. (In each case, the security mechanism would obviously be linked to a database containing details of authorised users.)

Another form of theft relates to the copying of programs and data resources in an organisation. Obtaining customer lists together with the details of the amount and type of business can obviously assist companies to encourage customers away from their competition. Theft of software is a major problem in the PC world where users often make illegal copies of the programs rather than purchase the package themselves – this practice is known as **software piracy.** This type of theft is more difficult to identify, since the original product has not physically disappeared as with the theft of computer hardware. Where software piracy is discovered, the owner of the computer on which the software resides (often the employer) is held to be legally responsible for the presence of pirated software.

The last category of computer theft covers the illegal use of computer time. In the past computer operators were often caught processing work for third parties or users were doing their own work at the office. Computer hackers spend their time searching for networks to which they can gain access. Having breached the security controls, they often browse around the databases in the installation but may not do any damage. In these instances, the only crime they can be charged with is the theft of computer time.

10.2 Security Beyond the Organisation

10.2.1 Hackers and Firewalls

Hackers are users from outside the organisation, who penetrate a computer system usually through its communication lines. Although some hackers are content merely to demonstrate that they have bypassed network security, there is a high risk of malicious damage to data, stealing of sensitive information (such as customers' credit card numbers) or entry of fraudulent transactions by the hacker. Hackers may also instigate a **denial-of-service** attack, in which a targeted web site is inundated with requests for information initiated by the hacker, rendering it inaccessible for genuine business customers.

A **firewall** is an additional system that enforces access control policy between two networks, especially between a corporate network and the Internet. The firewall monitors all external communications, checks user authorisation and maintains a log of all attempts to access the network. They can also be used to check for the presence of viruses, for the downloading of unauthorised software, and to guard against denial-of-service attacks.

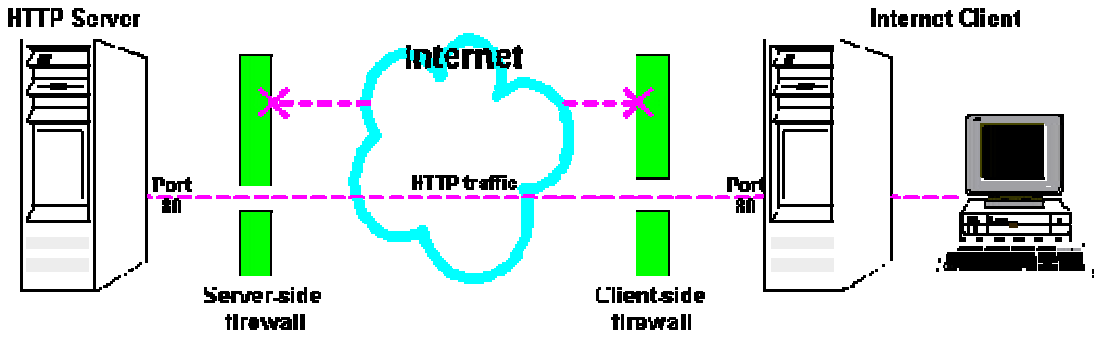

Figure 10-1. Diagram of a firewall (otn.oracle.com/products/ ias/daily/Aug20.html)

Data which is in the process of being communicated is also vulnerable to eavesdropping. **Encryption**, which scrambles data into an unreadable form, can be used to improve data privacy and prevent any unauthorised changes to the message, as well as protecting the confidentiality of data within the organisation.

10.2.2 Viruses

A computer **virus** is a program that invades a computer system, normally by residing in corrupt files. The virus has the ability to replicate itself and so spread to other files and computer systems. Some viruses are benign and merely advertise their presence, but others corrupt the files they infect and even destroy entire databases.

There are three main types of viruses. The original viruses were mainly systems viruses. They resided in the boot sector of a disk (the first place the computer looks when loading the operating system) or in the operating system utilities. These viruses were usually easy to find and clean. One problem was that they loaded into memory as soon as an infected machine was switched on and could often hide themselves from the anti-viral software.

The next generation of viruses attached themselves to executable files. When an infected program is run, the virus resides in memory and infects all new programs run until the system is switched off. These viruses are difficult to counter, especially on a network as common files are often infected. Even when the file server is cleared of infected programs, users have copies on their personal hard drives, or a infected copy of the program in memory when the virus check is performed on the server.

One area most users with which felt safe was the accessing of non-executable files such as word processing documents. Unfortunately there are now a number of *macro viruses* that can attach themselves to documents and spreadsheets. Even receiving a simple letter as an e-mail attachment can infect your machine. Some of the more well known viruses include:

- ***Michelangelo***. This virus infected many machines in the early months of 1992. The virus was primed to activate on Michelango's birthday (6th March) and had the capability of destroying all files on the hard disk of infected PC's. News of the virus made headlines and many businessmen and home users rushed out to purchase programs to check and clean viruses from their installations. On the day, some infections did occur but the main winners were the vendors of virus detection software.

- ***Stoned***. A very common virus in the late 1980's it came in many forms, some harmless while others corrupted files by attacking the directories and allocation tables. The main theme of the virus was to legalise the smoking of cannabis and normally the message "Your PC is now Stoned" would appear on the screen.

- ***Jerusalem***. Deletes all programs that are run on Friday 13th.

- ***Concept***. A macro virus, attached to word processing documents.

- ***EXEBUG***. A nasty little bug that may corrupt your hard drive. This is a systems virus and can infect the CMOS of your PC. Very difficult to find and eradicate as it uses "stealth" technology to hide from virus checkers.

With increasing globalisation and interorganisational communications, viruses are able to spread faster and further than ever before. Recent examples include Melissa, ILoveYou, and the Nimda virus, which make use of multiple methods of transmission. The real mystery about viruses is why they exist at all. Some experts suggest that computer hackers are motivated by the challenge of "beating the system" by writing programs that can bypass virus protection systems and take control of each individual machine. A more likely motive is to induce computer users to purchase legal copies of software. The only real winners in the new world of computer viruses are the companies selling computer software.

In the early 1980's the illegal copying of PC software, or *software piracy* was rife as there was no real business advantage to purchasing the software (except a copy of the official reference manual). Today it is estimated that about 50% of the PC software used in the USA has been illegally copied and the situation in South Africa is likely to be worse. One of the major motivations for buying software rather than copying from a friend is that the shrink-wrapped product is guaranteed to be virus free.

The best line of defence against viruses is the regular use of up-to-date anti-virus software, which will scan files for viruses and remove them if found.

10.3 Operational Problems and Errors

Computers are often seen as "super humans" in that they can perform their tasks at high speed and great accuracy. However the computer has its own, very specific weaknesses.

10.3.1 Dependency

Dependency may become a problem at two levels. Firstly, users of on-line, real-time systems are often totally reliant on the computer to perform their tasks. For example, visualise a busy Saturday at the local Pick 'n Pay supermarket when the back office computer malfunctions. All the point of sale terminals are linked to this machine to obtain price and other information and until the problem is fixed, no sales can be processed. Not a pleasant situation for shoppers and store managers alike. All organisations reliant on their computer to perform critical business activities must have a contingency plan to cover such emergencies, from the simple malfunction of a unit of hardware to a major disaster such as a fire in the computer installation.

At an individual level, employees who are accustomed to using a computer as a source of information, may lose confidence in their own judgement or decision-making abilities. When the computer is offline then all business activities grind to a halt, even though many of those processes could have continued based on principles and procedures that are not power-dependent!

10.3.2 Illogical Processes

Most conventional computer programs are made up of simple commands to instruct the machine (expert systems being one exception). When a computer error occurs, it could be as a result of hardware malfunction or the corruption of data. However this seldom results in an incorrect report or enquiry as the hardware and software are designed to detect this loss of integrity and provide an appropriate response (stop processing or generate an error message). Computers do not make calculation errors or read the incorrect data. But we have all heard stories of customers receiving telephone bills for outrageous (and incorrect) amounts and banks transferring amounts to the wrong accounts. These problems invariably originate from errors made by computer users or errors in the programs written to control the process. While humans make mistakes, sometimes on a regular basis, they have the advantage of working intelligently (although this is not always obvious). A clerk in a manual debtors system will probably realise there is an error when the telephone bill is over R1,000,000 and will check the client's detailed records before dispatching the account. The computer blindly follows the instructions in the program. However we can provide the computer with some sensitivity to problems by adding reasonability checks. For example it could highlight all amounts that appear to be too large (or small) in an exception report for the supervisor to check prior to distribution.

The bottom line is that the information provided by a computer should be more accurate and reliable than output from a manual system, but much depends on the expertise of users and computer professionals in the development and operation of the system. One classic example of a computer error occurred when one of the authors was working in the computer department of a large oil company. A colleague made a change to the layout of the customer statement to add a place for comments to be included, and tested the change by putting in a "Happy Christmas and Prosperous New Year" message. Needless to say he forgot to remove the message for the next monthly run and 25,000 customers were wished "Happy Christmas" in the middle of July.

In a number of studies focused on threats to computer systems, the largest percentage of financial losses were not from computer crime (20%), disasters (15%) or sabotage (15%) but from employee ignorance or negligence (50%). Management is often focused on external threats and natural disasters but the threat is from within. The recommendations from this research highlighted the fact that motivated, well-trained and supervised employees will go a long way towards reducing computer problems in the work place.

10.4 Computer Monitoring and Privacy

One of the major advantages of commercial computers is that given a large quantity of data about the organisation's business activities, it can then analyse the data from many different perspectives and provide management with valuable information as to the status of the

operation. If people are part of this system, either as customers, employees or even operators, the computer can use the information at its disposal to report on the activities and performance of each individual. The question is, how far can this process go before it becomes an invasion of privacy?

10.4.1 Computer Monitoring

As transactions are processed in a computer system, the program could store the code of the operator in the transaction to record who performed the activity. At a later date we may want to check on some aspect of the transaction and could check which operator was on duty at the terminal. We could also take all the transactions over the month and summarise them by operator code to evaluate the amount of work done by each operator. We could also analyse the number of mistakes, and the times when operators logged into the system and logged out.

With the introduction of workflow systems where documents are scanned into the system and routed to various workers, there is some justification for monitoring the pace and progress of activity on the network. However there are negative aspects as well. Monitoring can be stressful to certain individuals and there is a school of thought that suggests that workers who are being monitored change their work patterns and work quicker rather than better (issues such as customer consideration may be ignored as they appear to waste valuable time).

This all sounds much like George Orwell's "1984", a book about a future world where every thought and action were watched by Big Brother. Currently, one of the major issues of conflict between workers and management in the USA is whether supervisors should be allowed to read e-mail addressed to their subordinates. When e-mail is transmitted across the country, its privacy is protected by law, but within a business, e-mail is held to be the property of the employer, since it was created during the employer's time and using the employer's resources.

10.4.2 Invasion of Privacy

The other side of the coin is where organisations obtain information about an individual and use it for commercial advantage. You may be surprised to find out how much information about you is stored in computers around the country. Your school and university will hold a lot of personal information. You will have applied for a job or two, opened a bank account, purchased a house and applied for water and electricity supplies. You will have a few insurance policies, be seeing a doctor and dentist, have an account at a number of stores and own both a regular and cell phone. All these organisations will have information about you, and some of this information could be classed as sensitive such as your overdrawn bank account and the time you were caught for driving under the influence (mentioned on your school report).

This information has value. Direct mail businesses would like to post you catalogues and flyers detailing their latest products; and credit bureaux can use the data to assess your credit standing. More sinisterly, bureaux specialising in computer data matching are buying data from many sources to create a complex profile for each individual.

Most countries now have strict privacy laws to protect their citizens. For example the Federal

Privacy Act in the USA states that:

- Individuals are free to determine what information is being held by an organisation
- They can prevent the use or distribution of their information to other organisations without their consent
- They can view, obtain copies and correct their information
- Information can be collected and used only for necessary and useful purposes
- Information must be kept current and accurate
- Safeguards must be provided to ensure the data is secure and not misused
- Individuals can institute claims for damages they suffer as a result of wilful or unintentional violations of these rights

Similar legislation was introduced in South Africa in 2002, giving all citizens the right to know what data has been stored about them, what it is being used for, and to insist that incorrect data be rectified.

Although many issues have been resolved and the rights entrenched in law, others are very topical, controversial and as yet undecided. One example is the debate as to whether there should be censorship on the Internet. Should the network be an open medium for the free exchange of ideas and information? Or should legislators take responsibility to regulate content and activities such as child pornography. The debate continues.

10.5 Computers and Unemployment

James Martin calculated that computer processing was about on a par with manual processing in terms of cost performance in 1978. Since then computer processors have doubled in power every two years with little or no increase in cost. If the motor industry had advanced at the same speed as computers over the past 50 years, a Rolls Royce would cost less than R10 and run for a year on a single tank of fuel. Obviously these advances have provided business with cheap, reliable processing power but they have also begun to impact on employment levels. Early growth in computer processing had little effect on jobs. The introduction of computer systems called for new skills as large amounts of data needed to be captured. While some of the repetitive transaction processing was now automated, clerical workers could now supervise and control the processing cycle. Computers were hailed as machines to take the drudgery out of work and in most cases this was so.

With today's widespread use of computers, there are a number of changes to employment patterns that are credited to the computer revolution.

As anticipated, the clerical workers in many companies are gradually becoming knowledge workers, requiring new skills to operate and manipulate computerised applications. The numbers of these employees has shrunk over time as computer applications propagate throughout the organisation.

The number of blue-collar workers (employees in the manufacturing function) is falling. In some cases this is a result of improved processes and productivity but the impact of

automation and the introduction of robotic assembly is also a factor.

The impact of computerisation is most felt in the area of middle management when sophisticated MIS and DSS systems have provided top management with easy access to information without the overhead of layers of supervisors and managers. The outcome of this change is a sharp reduction in the layers of management in most organisations and the arrival of large numbers of middle aged managers at the unemployment queues.

Opinions are mixed about the long-term effects of computerisation on employment. Some experts predict that job losses from technological advances are always offset by increased demand for skills in other areas. The jobs are there but some individuals may need re-training. The other side of the coin is that computer technology can improve productivity while reducing costs, and staff is often the major cost to the organisation. The new reality may be that more and more people will lose their jobs to computers as corporations fight to remain competitive.

10.6 South African Perspective

Spam is the equivalent of junk mail sent via the internet: electronic messages are sent automatically to computer-generated e-mail lists. The recently promulgated Electronic Communications and Transactions (ECT) Act of 2002 protects individuals against unwanted spam, by requiring any company that sends unsolicited commercial communications to provide the recipient with the option of being removed from the mailing list, and to disclose the source from which the his or her details were obtained.

During January 2003 the first charge was laid in terms of this section of the Act, against a marketing company which continued to send unsolicited emails after having been requested not to do so. Companies or persons found guilty of such an offence are liable for a fine or imprisonment for up to 12 months, but the cost to the taxpayer may be disproportionately high. In this case, since the charge was laid at a Johannesburg police station, and the marketing company is based in Cape Town, a search and seizure warrant would have to be issued in Johannesburg and sent to Cape Town for approval by a Cape Town magistrate, after which a member of the SAPS would carry out the warrant and obtain a copy of the company's database to be used as evidence. Although a successful conviction may act as a deterrent to other South African companies in the future, the global nature of the internet makes it virtually impossible to control electronic communications through legislation.

10.7 Beyond the Basics

Biometrics is the technique of electronically measuring a physical characteristic of an individual and automatically comparing that measurement with an equivalent value stored in a database, in order to identify the individual. Among the many physical characteristics that have been used for biometric measurement, the three that have given the most consistently successful results are retinal scanning, iris scanning and finger imaging.

Retinal scanning involves bouncing a beam of light off the back of the eyeball, using a scanning device that rotates six times per second to build up a map of the blood vessels that are present. The information is then digitised and stored in an easily retrievable database.

Although this technology requires close proximity of the individual to the scanning device, it provides a unique and stable method of identification. *Iris scanning* measures the arrangement of structures within the coloured circle that surrounds the pupil of the eye. It also provides a unique and permanent template, but is more demanding than other methods in term of equipment cost and memory requirements. *Finger imaging* is the 21st century implementation of the fingerprints that have been in use for decades, and is based on the generation of a unique byte code from the scanned image of a fingerprint. This technology still requires physical contact with the scanning equipment, and the results can be distorted by dirt or skin damage.

10.8 Exercises

10.8.1 Viruses

- The **Nimda worm** spread rapidly across computer networks during September 2001. Use the internet to find out three methods that it uses to infect computer systems.
- Suggest three precautions that you could take to reduce the risk of your PC becoming infected with a virus.
- Read the email message that follows, and then use the internet to find out whether such a virus actually exists.

From:
Subject: Urgent - Virus alert

Virus Planet!

To those who are using handphone !!

Dear all mobile phone's owners,

ATTENTION!!! NOW THERE IS A VIRUS ON MOBILE PHONE SYSTEM.

All mobile phone in DIGITAL system can be infected by this virus. If you receive a phone call and your phone display "UNAVAILABLE" on the screen (for most of digital mobile phones with a function to display in-coming call telephone number), DON'T ANSWER THE CALL. END THE CALL IMMEDIATELY!!! BECAUSE IF YOU ANSWER THE CALL, YOUR PHONE WILL BE INFECTED BY THIS VIRUS.

This virus will erase all IMIE and IMSI information from both your phone and your SIM card which will make your phone unable to connect with the telephone network. You will have to buy a new phone.

This information has been confirmed by both Motorola and Nokia.

For more information, please visit Motorola or Nokia web sites:

http://www.mot.com
http://www.nokia.com/

There are over 3 million mobile phone being infected by this virus

in USA now.

You can also check this news in CNN web site: http://www.cnn.com

CASE STUDY: CREAM ADVERTISING

Cream is a large and well-established advertising company, with corporate clients in all the major South African cities. Over the last decade, Cream has developed a reputation for the creation of avant-garde and witty advertising campaigns, predominantly on television and in glossy magazines, and has scooped several prestigious national awards. Much of their success is ascribed to the diversity of talents and personalities within the company, and a strong ethos of teamwork. A lot of time is spent in meetings and informal discussions between staff, and the pervading culture within the organisation is that work should be not only challenging but also fun.

Information technology is used to support various separate business functions:

- Accounting and administration, including the general ledger, accounts payable and receivable, and payroll.
- Graphic design for the development of new conceptual material.
- Word processing and presentation software for writing copy and making presentations to clients
- E-mail for communications and internet browsing to keep up with advertising trends.

Cream does not have an in-house IS department, and relies on the support provided by vendors and outside consultants to maintain their systems and solve any computer-related problems.

A brief overview of their business activities is as follows:

- The general manager, Jade Smith, contacts existing client by phone at least once a month to check that they are happy with the performance of their current campaigns, and perhaps make suggestions for future changes to content or media.

- All members of staff listen to industry gossip, and if a competitor's advertising campaign appears to be badly received, Jade is informed and decides whether to contact the client to market Cream instead. If so, she sets up an appointment for the marketing manager, Tim Mabusa, to give a standard presentation showing examples of previous work. Tim also provides a glossy brochure detailing the expertise and abilities within the firm, but his enthusiastic personality is a vital ingredient of the sales talk.

- When a new campaign is initiated, Jade will appoint one of her senior staff as project manager, and the two of them will meet with the client to discuss the form that the campaign should take (content, media, etc), and provide an initial (estimated) quotation. In many cases this meeting involves travel to other cities, which adds to costs and seriously impacts their availability for dealing with other business issues.

- A fee of 20% of the initial quote is payable before any further work on a new campaign is undertaken. A project team consisting of the project manager, a graphic designer and a copywriter will then work closely together to create several alternative ad outlines. These

are presented to the client for discussion and possible reworking before the final quote is submitted and production begins on the advertisement.

- Cream take care of all the liaison with publication media, and confirm to the client the periods and costs involved. The actual account for publication or broadcasting is submitted directly to the client, and Cream is not involved in the client's financial transactions other than the money charged by themselves for work done. Payment of the final quoted amount less the initial fee is due within 30 days of completion and invoicing.

As the business has grown, so more and more time is being spent on travel, telephone calls and faxes. A lot of coordination is needed to keep track of the various elements of each campaign, and make sure that actual advertising material, publication arrangements and accounting are all being attended to. Holdups frequently occur because the initial 20% fee has not yet been debited, or else it has been received but the project team have not been informed that they can proceed; and several TV ads have received unsatisfactory broadcast times because bookings were made late. Staff are tired rather than stimulated, and Jade is concerned that the quality of their work will be affected. She is wondering whether the introduction of additional technology to support the business processes would free her staff to focus more on their creative abilities.

(a) Give practical examples of how information systems could be used to support the business at each of the management levels.

(b) If you were Jade Smith, what business strategy would you select (low-cost, differentiation, or niche marketing) and why? How could IS be used to support this strategy?

(c) What opportunities would there be for the use of groupware, both within and beyond the company?

(d) In what ways could the implementation of e-commerce replace or enhance the existing business activities of Cream?

(e) A network infrastructure that supports e-commerce also exposes the organisation to added security risks. Suggest ways in which these risks could be minimised.

Section IV: IS Management

Since the birth of commercial computing, organisations have been developing computer applications to meet the needs of their users. Initially this process was almost entirely machine orientated since the high costs of computer hardware made it necessary to maximise the usage of this scarce resource.

Initially computers were used as sophisticated record keeping devices. As their price performance became more attractive so more and more secondary applications were found. Gradually each organisation's portfolio of computer applications has grown to the point that many could not function without the use of this electronic device. Organisations are using Information Systems to boost competitiveness and growth.

This transition has also seen the evolution of information architectures. Today's information processing environments tend to be integrated, decentralised and highly complex. They require detailed planning as to what hardware infrastructure should be established and which new applications should be developed. They require high quality systems to be developed as the maintenance load in some organisations is threatening to draw on all the resources of the IS department.

Advances in computer technology have resulted in computers becoming thousands of times faster, cheaper and therefore more productive than machines of the late 1950's. Unfortunately improvements achieved in the development of applications software have not kept pace, with the result that developing and maintaining in-house applications has become the major cost facing today's IS departments.

IS development projects require careful planning and the use of sophisticated tools with which to build new applications, and management techniques to ensure systems are delivered on time, within budget and to the user's expectations. The successful introduction of new systems also depends on the handling of change management within the organisation and the establishment of reliable procedures both for routine business activities and for coping with unexpected occurrences.

11. IS Planning & Acquisition

We know why organisations acquire new computer systems. In most instances computers are cheaper and more efficient than people when it comes to performing common, well defined tasks such as deciding when stock items should be reordered or generating customer statements. And as the productivity gap widens with each new advance in computer technology, new and innovative ways are being found to reduce costs through automation.

The question is "how does an organisation recognise the need for a new computer system?" Forces that highlight the need for change could come from the business environment (such as increased competition or new government regulations) or from within the business itself (for example where growth is beyond the capacity of the current system or new products are identified). Increasingly opportunities to automate arise through the introduction of new and innovative technology which can provide major cost reductions, improved management information and better service to customers. In most medium to large organisations there is a formal strategic planning process; and the new directions and changes identified in the 3 to 5 year business plan will enable the organisation to identify the computer systems required to support these applications in the future.

Once the need for a new system has been identified, plans must be developed to ensure that the new system can be successfully integrated with existing business processes, and that it will provide an acceptable return on investment for the organisation. Finally, effective project management is essential if systems are to be produced that correctly fulfil the requirements of their users without exceeding the constraints of time and budget.

11.1 Frameworks for Analysing Information Systems

There are many frameworks for analysing and studying information systems. Many of the commercially inspired frameworks are tied to a specific *system methodology*: they are very specific, often proprietary, approaches to analysing information needs, designing and developing information systems that address these needs. In addition, there have been many academic frameworks developed, each suitable for specific types of analysis e.g. strategic planning, comparative analysis, historical analysis, etc.

To give you an idea of these frameworks, we give you three examples.

11.1.1 Value chain analysis

In value chain analysis, the organisation is seen as a large input-output system, in which the inputs are the raw materials or services brought into the organisation, which are processed in some way, marketed and sold as outputs. Each point of this chain is analysed to uncover opportunities where value can be added or costs reduced. Although the complete model of the value chain usually includes both primary and support activities, the greatest level of return can be expected through the implementation of IS within the primary activities.

- **Inbound logistics** include the receiving, warehousing, and inventory control of input materials.

- **Operations** are the value-creating activities that transform the inputs into the final product.
- **Outbound logistics** are the activities required to get the finished product to the customer, including warehousing, order fulfillment, etc.
- **Marketing & Sales** are those activities associated with getting buyers to purchase the product, including channel selection, advertising, pricing, etc.
- **Service** activities are those that maintain and enhance the product's value including customer support, repair services, etc.

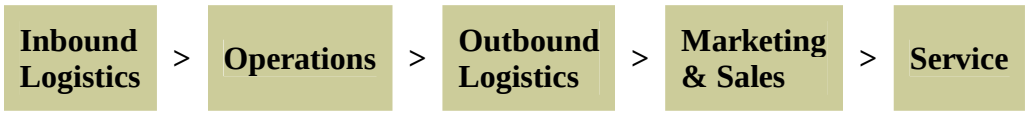

Figure 11-1. Primary activities within the value chain

11.1.2 The Zachman Framework

Zachman developed a framework aimed at a more systematic delivery of information systems, modelled loosely on the way buildings are constructed from an architectural point of view. According to Zachman, information systems need to be considered from six different perspectives (or dimensions).

- **Data:** which data *entities* do you want to capture and what are the *relationships* between these entities?
- **Function:** which (business) *functions* need to be addressed and which *arguments* does each function have?
- **Network**: which *nodes* need to be supported and what *links* exist between them?
- **People**: who are your *agents* and what are their *tasks* or *work*?
- **Time**. *when* do things happen and to which *cycles* do they conform?
- **Motivation:** what are the *ends* or goals and by what *means* will you get there?

Each of these dimensions is then examined at a number of different levels, to identify the system requirements and how they can best be implemented.

11.1.3 Strategic Importance Grid

The strategic importance grid looks at the entire information systems portfolio of an organisation i.e. all the systems currently in operation as well as the future systems currently under development or being planned. The critical focus of this framework is the assessment of whether a significant portion of an organisation’s systems is of a strategic nature and classifies the organisation accordingly into one of four possible categories on the IS strategic importance grid as shown in figure 11-2.

	Systems Currently in Operation	Systems under Development/ Being Planned
Predominantly of a Strategic Nature	STRATEGIC	TURN-AROUND
Predominantly of an Operational Nature	FACTORY	SUPPORT

Figure 11-2: Strategic importance grid

The main use of this table is to assess the importance of the IS strategic planning in the overall strategic business plan. It can also be of use when doing strategic competitor analysis or when assessing significant shifts in IT budgets. Try to find an example of a South African company for each of the four categories. As you try to place these examples, you will notice that the boundaries between the cells are not definitive: some companies will occupy boundary positions between cells whereas others will fit a certain category almost perfectly.

11.2 IS Planning

The various components of an organisation's information systems (hardware, software, databases, networks, and people) need to be successfully integrated in order to provide the right information at the right place and time. This is not going to happen by accident. An ***IS architecture*** is needed to define the IS resources that will be used to support the business strategy, and the standards that should be adhered to in order to ensure compatibility within the system.

The starting point for IS planning should be the clear identification of the application needs of the business, based on the information that is required by management. The activities that are managed by the IS department, such as the prioritising and scheduling of system development projects, must be in line with overall business goals. Alternative software products and acquisition options need to be evaluated before a decision can be made about the hardware and operating system that would be most appropriate.

Computer hardware should then be assessed on the basis of its compatibility with existing and future systems, its expandability and reliability. Other important issues include the availability of technical support, estimation of operating costs, and the financing method (e.g. leasing or buying) that is to be used.

11.2.1 Cost-benefit analysis

Cost-benefit analysis can be used to assess and prioritise new system development projects, by measuring the financial impact of proposed systems. Tangible benefits could include reduced inventory and administration costs, higher processing volumes, reduction of bad debts and improved cash flow. Intangible benefits such as improved customer satisfaction and better decision-making are more difficult to measure, but could be of significant value.

Typical costs that have to be considered in evaluating projects are

- Development costs, including staff training and conversion from the previous system
- Equipment costs, including space and air-conditioning requirements
- Operating costs such as staffing, insurance and power.

The reason for undertaking a cost-benefit analysis is to ensure that over the lifetime of the system, its benefits will exceed its costs, even though costs are likely to exceed benefits during the initial stages. The calculation must take into account the time-value of money (net present value) when determining the break-even point for the system, since interest would be earned (or saved) on the capital that will be invested in the project.

11.2.2 Funding of IS

The are three basic options available for the funding of an organisation's information systems: as an unallocated cost centre, as a cost centre, or as a profit centre.

The traditional model of an **unallocated cost centre** means that IS is regarded as an organisational cost, for which an annual budget is allocated in order to meet the costs of system development and maintenance. Other departments are likely to have little influence over the spending of the IS budget, the prioritising of projects and the standard of service that is delivered.

When the IS department operates as an **allocated cost centre**, then internal accounting is used to allocate IS costs to the departments using them. This makes it easier to identify areas of demand within the organisation, and may reduce the number of requests for (unnecessary) projects.

A **profit centre** approach means that the IS department must compete with outside vendors in providing IS services to the organisation. This often results in increased efficiency of the IS department, but may reduce the time spent on less profitable developmental work, reducing the ability to provide innovative and potentially strategic IS capabilities.

11.3 Software Acquisition Options

11.3.1 In-house development

Most large organisations have their own IS department, which is responsible for the development and support of the computer systems used to support the company's strategic goals. The methods commonly used during ***in-house development*** are covered in detail in the next chapter. However, this approach depends on highly skilled employees, and because of the time and cost involved, it often results in a backlog of projects awaiting development. If IS staff do not have the necessary technical expertise, or are too busy to attend to low priority projects, then alternative system development methods may need to be considered.

11.3.2 Commercial packages

The acquisition of off-the-shelf ***software packages*** provides a low-cost alternative to in-house