UNIVERSITY
OF LONDON

Information systems: foundations of e-business Volume 2

R. Shipsey

CO1108

2010

Undergraduate study in
Computing and related programmes

Goldsmiths
UNIVERSITY OF LONDON

This guide was prepared for the University of London by:

R. Shipsey

This is one of a series of subject guides published by the University. We regret that due to pressure of work the author is unable to enter into any correspondence relating to, or arising from, the guide. If you have any comments on this subject guide, favourable or unfavourable, please use the form at the back of this guide.

In this and other publications you may see references to the 'University of London International Programmes', which was the name of the University's flexible and distance learning arm until 2018. It is now known simply as the 'University of London', which better reflects the academic award our students are working towards. The change in name will be incorporated into our materials as they are revised.

University of London
Publications Office
32 Russell Square
London WC1B 5DN
United Kingdom

london.ac.uk

Published by: University of London

Contents

Introduction

The second volume of this subject guide is a continuation of the first volume. You will need to make sure that you have finished working through Volume 1 before you start work on these chapters. You may also like to read the Introduction to Volume 1 again for general information, for example, relating to the examination. The essential and additional reading lists are the same and are reproduced below.

In Volume 1, we studied the role that information systems play in organisations and in particular e-commerce companies today. We discussed business processes and how different types of information system can be used to aid different types of business processes. We discussed organisations in terms of the environment in which they operate and how information systems can be used to provide a competitive advantage. We considered the moral and ethical issues raised by the increased use of technology. We looked at the growth of e-commerce and considered the advantages and disadvantages of e-commerce compared to traditional businesses.

In this volume of the guide, we will discuss in detail the individual components that make up an IT infrastructure. We will look at the issue of information management and databases. We will discuss the evolution of telecommunications from dial up modems to wireless networks. We will consider the importance of information security and the steps that can be taken to achieve this. Finally we will discuss traditional and alternative methods for developing information systems. Outlines of the five chapters in this volume are given below.

As in Volume 1, each chapter includes learning activities and chapter questions which can be used to test your understanding and give you the opportunity to find examples and illustrations to use when answering your coursework and examination questions.

An examination paper (with example solutions) is included at the end of this guide so that you can see the type and level of questions to expect in the examination.

Essential reading

The subject guide is based on following book:

Laudon, K. and J.Laudon *Management Information Systems: Managing the Digital Firm* (Pearson, 2010) eleventh edition [ISBN-13: 978-0-13-609368-8](pbk)

Material in Laudon and Laudon is examinable. You should also be aware that rapid developments in the world of technology mean that neither the subject guide nor the recommended text can ever be completely up-to-date. You are therefore advised to access further reading wherever possible to keep abreast of the current state of technology available.

Following is a list of books that are recommended. By no means do you need to have copies of all of these books but a selection of your choice would complement the material covered in the subject. Some of these textbooks are very expensive and so I have given Internet addresses for additional reading wherever possible. You should also find your own additional reading by using a search engine to find appropriate material when possible.

Additional reading

Oz, Effy, *Management Information Systems* (Course Technology, 2008) sixth edition

[ISBN-13 978-1323901785](hbk)

Turban, E. and L. Volonino *Information Technology for Management – Transforming Organizations in the Digital Economy* (Wiley, 2010) seventh edition [ISBN: 978-0-470-40032-6] (pbk). See also http://bcs.wiley.com/he-bcs/Books?action=index&itemId=0470400323&bcsId=4953 for the student companion site for this textbook which is free to access.

Schneier, Bruce, *Secrets and Lies, Digital Security in a Networked World*, ISBN-13: 978-0471453802 John Wiley & Sons (23 Jan 2004)

See Steven Alter's website at www.stevenalter.com for some interesting articles and links.

See Wikipedia for a great example of a wiki as well as lots of useful information. Note however that material on Wikipedia is not guaranteed to be accurate and you should double check references from here using another source. http://en.wikipedia.org/wiki/

Guide to chapters

- In **Chapter 6** we describe the individual components (hardware, software and services) that make up an IT infrastructure. We will see how, and why, these components have evolved over the past 40 years, and look to the future to see what might happen next.
- In **Chapter 7** we will look in more detail at how data can be stored and managed effectively to produce meaningful information. We will consider some of the problems that can occur with traditional data storage and discuss how Database Management Systems can be used minimise these problems.
- In **Chapter 8** we will discuss the evolution of telecommunications technology and the role that it plays in an e-commerce business. We will describe the component parts and layout of different networks for use in business or personal settings.
- In **Chapter 9** we discuss the security of computers, networks and the information that is stored and transmitted by them. We will consider various threats to information and computer security and the steps that companies and individuals can take to make themselves less vulnerable to these threats.
- In **Chapter 10** we will look at the methods that companies can use to develop new and existing information systems. We will compare the traditional structured approach with alternative methods of development and discuss the advantages and disadvantages of each method.

Volumes 1 and 2 of the subject guide each contain about half of the course material, so you are now already half way through 2910108. Congratulations on getting this far – keep up the hard work and good luck with the examination.

Chapter 6

IT Infrastructure

6.1 Introduction

In this chapter, we describe the components of an IT infrastructure. We will see how quickly and by how much technology has changed over the past few years. We will consider what has driven this change, and the implications that it has for managers who are trying to keep their organisations in line with ever changing technology trends. We will describe some of the newest hardware and software applications and discuss how they can be used to help organisations meet the growing demands of their customers, employees, business partners and suppliers.

Essential reading

Laudon and Laudon, *Management Information Systems Managing the Digital Firm*, Chapter 5.

Additional reading

Turban and Volonino Technical Guides 1 (Hardware) and 2 (Software) from the student companion website for *Information Technology for Management*. This can be found at http://bcs.wiley.com/he-bcs/Books?action=resource&bcsId=4953&itemId=0470400323&resourceId=17218&chapterId=48688.

Moore, Gordon, *Cramming more components onto integrated circuits*. This paper can be found at ftp://download.intel.com/research/silicon/moorespaper.pdf.

6.2 Learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe the seven major components that make up an IT infrastructure
- discuss the evolution of IT over the past 30 years since the first commercial use of mainstream computers to the present day
- describe the factors, including Moore's law and Meltcalfe'e law, that have driven the rapid evolution of technology
- outline the emerging hardware trends including mobile devices, grid computing, cloud computing, autonomic computing, virtualisation and multi-core processors
- outline the emerging software trends including Linux and other open-source software, Java, Ajax, Web service and applications

- understand the considerations that managers have to take into account when deciding upon an IT infrastructure for their organisation
- discuss the elements that make up the total cost of ownership of an IT infrastructure.

6.3 What is an infrastructure?

An IT infrastructure can be viewed (incorrectly) as the hardware and software that make up an organisation's information system. The reality is more complex than that. Over and above the hardware and software, there are a range of different services needed to make an organisation's IT systems come alive. So IT infrastructure is really a combination of hardware, software and services.

The services that we are talking about include:

- purchasing (procurement), setting up (installing) and supporting (when problems occur) a networked IT system that meets the needs of the organisation
- providing the relevant training and research facilities to ensure that the IT system remains fit for purpose and can be used effectively by employees
- deciding on how the capacity of the systems (including data management systems) can be used to an organisations advantage.

Learning activity

Think about a large multi-national organisation and a small local organisation. How do the IT services provided/required by the IT infrastructure of the large organisation differ from the IT infrastructures of the smaller organisation?

6.4 How IT infrastructure has evolved

The principal developments in IT infrastructure can be summarised as follows:

- **Mainframe computers (1959 to present day)** – the emergence of mainframe computers marked the beginning of the widespread commercial use of computers. IBM have always dominated this market. Mainframe computers were under the control of professional programmers and systems operators and were highly centralised. As they developed, mainframe computers become powerful enough to support hundreds of online remote terminals connected to the centralised mainframe. With the advent of the personal computer, many people thought in the 1980s that mainframes would cease to exist. However, their ability to store and process huge amounts of data means that mainframes are still an important component of many IT infrastructures.
- **Personal computers (1981 to present day)** – people have gradually started to have computers in their homes, to the extent that it is now quite unusual for someone in the developed world not to have access to a computer. The rise of the personal home computer has driven the need for employers to keep up and provide personal computers in the work place too. Microsoft Windows has

dominated the personal computer but open source software such as Linux, which is not only free but also good, is starting to challenge this domination.

- **Client/server networks (1983 to present day)** – as personal computers and laptops become cheaper, organisations started to replace their mainframe terminals with PCs linked together in a network. At the heart of the network of PCs (**clients**) is a **server** (which might be a mainframe or a powerful PC) which stores some of the data, applications software and other instructions that the network users need in order to communicate and process transactions on the network. There are different types of servers. A **web server** provides web pages to users, an **application server** assigns specific tasks to other servers to enable a faster more efficient response to client requests than a single mainframe trying to do everything. Large organisations use a **multi-tiered client/server architecture** that has several different levels of servers.
- **Enterprise Internet computing (1992 to present day)** – the rise of the Internet has meant that the last 18 years have seen an explosive growth in the functionality and popularity of computers. The Internet has developed into a trusted communications tool and organisations use the Transmissions Control Protocol/Internet Protocol (TCP/IP) networking standard to link their networks together. Different types of hardware, software and services can be integrated to provide an enterprise-wide network.
- **Cloud computing (2000 to present day)** – the concept of cloud computing almost takes us back to the idea of the mainframe. Massive computing centres are owned by companies such as Google, IBM and Microsoft. The *Google cloud* for example contains thousands if not millions of cheap servers which store huge amounts of data. This means that we can search for and find the answer to a question in seconds. When an individual server dies it can be replaced with the latest model meaning that the whole system is continually being upgraded and never ages.[1]

Learning activity

Write a paragraph discussing the similarities and the differences between the mainframe era and the cloud computing era.

6.4.1 What is driving the change in IT infrastructure?

As you can see from the previous pages, IT infrastructure has evolved a great deal in the last 20 years. Here are some of the reasons why this has happened:

Moore's Law

Moore's Law[2] says that

[1] See an article entitled *Google and the Wisdom of Clouds* by Stephen Baker at $http://www.businessweek.com/magazine/content/07_52/b4064048925836.htm$ for more information on Google and the concept of cloud computing.

[2] Moore's Law is named after Dr Gordon E. Moore due to his paper entitled *Cramming more components onto integrated circuits* which was published in 1965. Download the original paper from ftp://download.intel.com/research/silicon/moorespaper.pdf.

The number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years.

There are variations on Moore's Law (not actually stated by Moore himself) which say that:

- The power of microprocessors doubles every 18 months.
- Computing power doubles every 18 months.
- The price of computing halves every 18 months.

Whichever variation of Moore's law you look at, this is exponential growth (or in the case of price decline) and means that if 2,000 transistors were possible in 1971 over a billion are possible now. Figure 6.1 illustrates the exponential growth of computing power over the years.

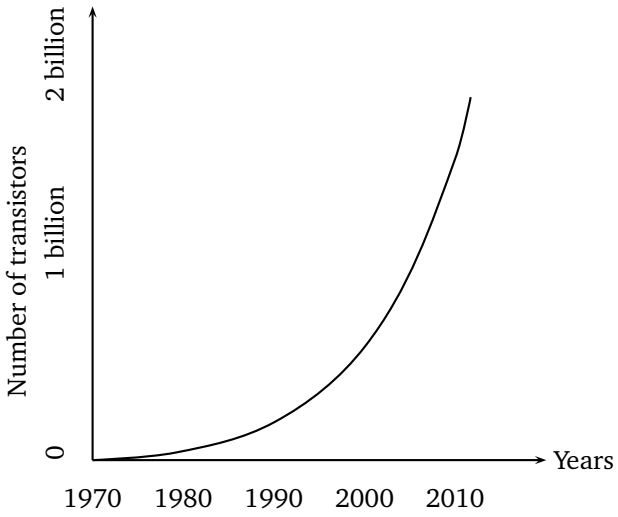


Figure 6.1: Moore's law describes the growth in computing power over the years

Nanotechnology is promising to continue this trend into the future.

Learning activity

Do some research on the Internet to learn about Nanotechnology and write a short essay explaining what this technology is and the changes to computing that it will bring about.

Digital storage

As it becomes possible to store more and more material (photos, video, music etc as well as text files) digitally, so the demand to store more increases. However much data storage is possible, users will always fill it and demand more.

Metcalfe's Law

Metcalfe's law says that

> *The value of a telecommunications network is proportional to the square of the number of connected users of the system.*

What this means is that if you have two telephones you have one connection, but if you have ten telephones then you have 45 connections. This is illustrated in figure 6.2

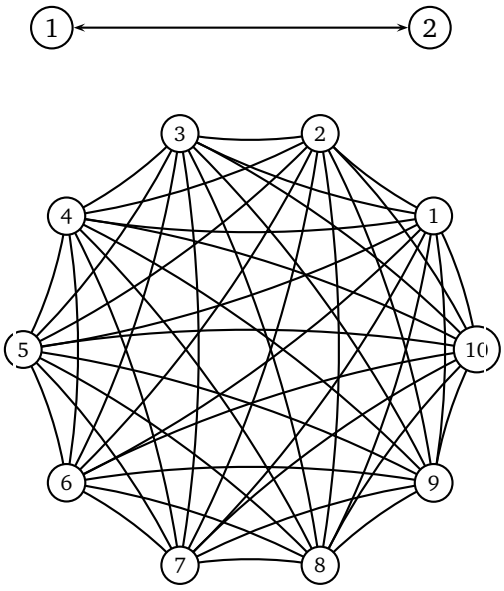


Figure 6.2: Two users = one connections; ten users = 45 connections

The same is true in terms of computer networks and the result is that if you add one more computer to an existing network that is fairly inexpensive, but the resulting benefits (in terms of the number of new connections) is great.

Learning activity

- Suppose an existing computer network has ten users and therefore 45 connections as in the diagram above. An eleventh user is added and connected to all of the other ten users, how many connections are there now?

- Suppose two networks each consisting of ten users are merged so that the 20 users can all communicate directly with each other. How many connections are there now?

Declining costs

It is getting cheaper every day for people to connect to the Internet because of declining communication costs. As more and more users connect to the Internet, organisations must find ways to meet their expectations and demands. The Internet is one of the biggest drivers in the exploding use of computers both in the workplace and the home.

Improved standards

The Internet has been able to grow because technology has been developed which allows products to work with each other. Users rely on the interoperability of products.

6.5 Components of an IT infrastructure

There are seven major components of an IT infrastructure. The aim is to make these components all work seamlessly together to make an enterprise system that works anytime, anywhere.

1. **Computer hardware**

   The physical components (a personal computer, server, laptop etc) perhaps made by IBM, HP, Dell or Sun Microsystems, and containing a microprocessor, the heart of any computing device, probably made by Intel, AMD or IBM.

2. **Operating system**

   Computers need to know what, when and how to do things and it is the operating system that tells them. Operations such as logging-on, file management and network connectivity are controlled by the operating system. Microsoft Windows, in one or other of its versions, is by far the most prolific operating system. However Unix and Linux, which are often associated with large networks because they require less application overheads and have faster processing, are also available for PCs. Linux open-source software is becoming the operating system of choice for organisations looking to reduce their costs because it is free and reliable.[3]

3. **Enterprise software**

   The aim of enterprise software applications is to integrate applications into seamless processes across the organisation. Customer relationship management and supply chain management systems (see volume 1, chapter 2) are the two most popular applications in this category. Thanks to the proliferation of networks, these applications are becoming popular and affordable for even small- and medium-sized organisations.

4. **Data management and storage**

   More and more data, on customers, employees and the business itself, is being gathered by organisations. Storing and managing this data so that it is easily accessible and provides meaningful information is extremely important. **Storage area networks (SANs)** provide an economical way to consolidate data from

[3] I am a big fan of Linux and would encourage you to look at the Linux website $http://www.linux.org/$ and consider trying Linux for yourself.

across all of the systems within an organisation. Online users want instant access to data and SANs help organisations to provide it deliver this.

5. **Networking/Telecommunications**

   As we progress towards the convergence of all things digital, networking and telecommunications are merging into one. Instead of having one platform for networking computing devices, and another for telecommunications, there are now companies who provide a combination of telephone services, mobile phone connectivity, computers and peripheral devices, handheld PDAs and wireless services as one digital package.

Learning activity

Who is the main provider of networking and telecommunications in your country? What digital packages do they provide?

---

6. **Internet tools**

   The Internet continues to expand the services that organisations are able to provide to their employees, customers, suppliers and business partners. Intranets and extranets which are built using existing Internet technologies give organisations an easy and inexpensive method of providing services that were prohibited by cost only a few years ago.

   Rather than buying all of the hardware necessary to support websites, intranets and extranets, many smaller companies choose to use web hosting services instead. These provide the hardware, software, expertise and security necessary for a company to have a web presence without becoming a major distraction (in terms of time and money) from the core business.

7. **Consultancy and system integration**

   The systems used in many medium- and large-sized organisations are too complex for the organisation to manage them on their own. Integration services provided by companies such as IBM and Hewlett-Packard are necessary to keep everything working and up to date. It makes sense for a company which, for example, specialises in making clothes, to concentrate on making clothes and allow a company which specialises in computers to keep their computer systems in good shape.

   As organisations gradually update their old computer systems, which might be 20 years old, with newer technology, the old and the new must work together. Organisations generally cannot afford to simply throw out all of their old technology and replace it. It is cheaper (and involves less staff training) to use middleware and other technologies which integrate the old and the new.

6.6 Hardware and software development

IT infrastructure components such as storage and telecommunications are getting cheaper and cheaper and yet organisations are spending more and more on information technology. Why is that? The answer is that users are demanding better, faster, easier ways to use computers and communicate with others.

In this section we will have a brief look at some of the newer hardware and software technologies that are helping organisations to meet the growing demands of their customers, employees, suppliers and business partners.

6.6.1 New Hardware

Most of these hardware components are at a comparatively early stage in their development. As hardware technologies improve, it is likely that these developments will play a big part in the the information systems of the future.

The mobile digital platform

Computer users now expect to be able to use their devices anytime anywhere, 24/7, 365 days of the year. Technology manufacturers are meeting this demand with new communication devices such as mobile phones, smartphones and netbooks. A netbook is built specifically for wireless communications and Internet access. Small in size, relatively inexpensive compared with laptops, and with decent processors, memory and hard drives, analysts expect the popularity of netbooks to continue to rise.

Grid computing

Grid computing means connecting computers into a single network to create a virtual supercomputer. The individual computers don't have to be anywhere near each other and can be used for other things when they are not part of the grid.[4] Combing all the idle time of millions of computers into a continuous, connected, computing capacity gives you a supercomputer with immense speed and flexibility, at a fraction of the cost of buying a supercomputer.

Cloud computing

Most organisations do not provide their own utilities such as water or electricity. Instead they buy them in from a centralised source – the water company or the electricity company. They rely on the provider to increase supply whenever they increase demand.

Cloud computing, also known as **on-demand computing** or **utility computing** is similar to other utilities. They provide computing facilities to companies from a centralised source and meet increased demand when necessary (for example Internet shops require greater capacity over the run up to Christmas than at other periods in the year). This is cheaper for the organisation as they do not have to own as much IT technology as they would have to in order to meet the demand at their busiest periods. It also enables organisations to expand and develop the services they provide without first having to buy all of the necessary hardware and software.

There are some disadvantages to cloud computing. What happens for instance if the utility providers' servers go down?

[4]For example, the RSA challenge involved factorising a large composite number. This is a very hard problem requiring a supercomputer. One method used was to allow individuals to sign up and let their computer be used, when they weren't using it themselves such as throughout the night, as part of a grid.

Autonomic computing

As organisations rely more and more heavily on IT to meet the demands of their customers, they cannot afford to have any system 'downtime' – it is too expensive. Autonomic computing is a step towards creating an IT infrastructure that is able to diagnose and fix problems with very little human intervention.

This type of computing is still very new, but if autonomic computers can configure themselves, optimise and tune themselves, fix themselves when broken, and protect themselves from intruders and self-destruction, then they promise to help many organisations who are struggling to maintain complex IT infrastructures.

Virtualisation

As computers get cheaper, organisations tend to buy more and more rather than optimising the use of their existing hardware. This can mean for example, that an organisation has ten servers running ten different applications. The ten servers are running all of the time, but each is being used for a small part of the time. It is much more cost and energy efficient to run the ten applications on one server, choosing which application is needed at any one time. This is what *virtualisation* is about. It means running multiple operating systems and application programs on one machine and increasing the overall utilisation rate of that machine.

It is now possible to get **multicore processors** which have two or more processors rather than a single chip on a single processing core. This reduces the overall number of servers or processors required, thereby reducing the total costs of ownership and running costs such as electricity.

6.6.2 New software

You might have all of the hardware that money can buy, but without the right software it's not much use. Here we will look at existing and emerging software that is trying to get the most out of hardware.

Linux and open-source software

Linux is a Unix-like operating system originally written by a Finnish post graduate student called Linus Torvalds. Torvalds wanted to build an operating system that anyone could download from the Internet, no one would own, and thousands of people could develop.[5] *Linux* has grown rapidly as its small size and low cost make it ideal for information appliances. It is also less prone to crash than most other operating systems and this makes it very attractive to companies running e-commerce Internet businesses.

Other open-source software includes the *Mozilla Firefox* web browser and free office software *OpenOffice*. Open-source software generally tends to be more secure than other leading software programs because of the number of people who are involved

[5] The latest free version of Linux, Ubuntu 9.10, was released in October 2009. You can download it from http://www.ubuntu.com/.

in developing the programs – because the software is open source anyone who is interested can get involved, spot bugs and make improvements.

Software for the web: Java and Ajax

Java meets the need for interactive programming over the Internet. This programming language is operating system and processor independent, there is no need to worry about compatibility between Windows, Macintosh or UNIX. Previously it has been almost impossible to share data between various hardware and software platforms. Many large mainframes could not pass data to small PCs without special programs, and data used in individual PCs could not be passed to larger information systems.

Java solves many of these problems by creating *Java applets*. These are miniature programs which perform very small, specialised tasks one at a time. When a user wants to perform a task, the coding for it is moved from the server where it is permanently stored and executed on the client (user) computer. When the task is complete, the code is removed from the client computer. This reduces storage needs on the client computer. This means that applications can be run on small computing devices that do not have the capacity to hold large software programs.

Many websites require some form of interaction. For example, you might pay a bill, renew your driver's licence or complete your tax return online. A new technique that enables and improves these interactive processes is a combination of Asynchronous Javascript and XML languages called **Ajax**. Ajax works in the background of interactive web pages, exchanging small pieces of data that make web based processes run smoothly.

Web services

Web services use Internet technology to link application programs together. As they are web-based, they can be used across traditional organisational boundaries extending to customers, suppliers and business partners. The main advantage of web services is their reuseability – one web service can be used by many different organisations. Examples of web services include:

- MySpace and Facebook – social networking sites.
- Flickr – for photo sharing.
- Winkball – for video messaging.
- Google – for Internet searching.

As the Internet is used for more and more applications, computer languages are evolving to keep up. **HTML** (HyperText Markup Language) works well for displaying text and graphics, but current computing applications demand more than this. The following software standards and communication protocols provide easy access to data and information via Web services.

- **XML** (eXtensible Markup Language) is designed to control the data on a web page, making it more manageable.
- **XHTML** (eXtensible HyperText Markup Language) combines HTML with XML to create a powerful tool for building web pages.

- **SOAP** (Simple Object Access Protocol) allows applications to exchange data and instructions.
- **WSDL** (Web Service Description Language) describes a web service so that other applications can use it.
- **UDDI** (Universal Description, Discovery and Integration) lists web services in a directory so that users can find them.

Mashups and widgets

Mashups combine separate applications into one. For example, combining a mapping service with a store locator results in a map with stores locations shown on it.

Widgets are small software programs that you can add to a website or even to your own desktop to provide additional functionality. A widget might be useful (for example allowing you to run a slide show on your web page) or simply for fun (for example allowing you to send your friends a virtual drink).

Software outsourcing

Earlier we described how organisations can go to utility companies to meet their hardware needs (see section 6.6.1). The same is true for software. Other than developing their own software, organisations can meet their software needs by:

- buying software packages from a vendor;
- buying software as a service;
- outsourcing their customised software development needs.

6.7 Management issues

Keeping up with all the changes in technological speed and ability, and making wise decisions is a difficult task for the managers of an organisation. There are many questions that need to be answered.

6.7.1 Who should manage what?

As users (and employees) become more familiar and comfortable with technology, they usually see it as a helpful tool which aids their work. Sometimes this can lead to conflict in the organisation as there is disagreement about who should manage the IT infrastructure. Should there be a highly centralised control that provides a secure and cohesive computing environment, but potentially hinders the ability of users to get the job done? Alternatively, should there be a decentralised governance of IT that allows employees to set up their workstations however they like? This is more flexible but could lead to a stack of problems with compatibility issues, problems providing support for different operating systems and so on. There is no right or wrong answer – managers have to decide what the right approach is for their organisation.

6.7.2 What IT infrastructure should we invest in?

In order to meet the needs of their customers, employees, suppliers and business partners, organisations are having to rethink their strategic models for creating, processing, storing and delivering data. In particular, companies which interact with their customers via the Internet, which is available 24/7, need a model incorporating hardware, software and data that is also available 24/7. If a company fails to keep up with trends and demands then they risk losing business and hence revenue. Easy Internet access for customers and ease of entry into the Internet market by competitors means that customers can simply go elsewhere if the company does not adjust to meet current consumer demands.

Is it scalable?

It is hard for an organisation to know how much computing capacity they will require in the future. Managers need to design **scalability** into their IT systems to avoid under-building or over-building. The idea is to build the system to meet capacity for what the organisation thinks it needs, but to allow in the design, for the easy increasing of capacity if the system is more successful than was originally thought. Similarly, it should be easy to decrease capacity if the system is not as successful as intended so that the organisation is not left with a lot of unused and expensive equipment.

Are we spending the correct amount on IT?

If the organisation spends too little on IT infrastructure they are in danger of missing opportunities for improved products and services. On the other hand, if they spend too much on their IT infrastructure, they may be wasting resources that could be better used elsewhere. The following tasks can be carried out to help the company see where it stands.

- Make an inventory of the market demands for the company's products or services.
- Analyse the company's five-year business strategy.
- Examine the company's IT strategy, infrastructure and costs for the next five years.
- Determine where the company fits between old technologies and brand new ones.
- Benchmark the service levels of the company against its competitors.
- Benchmark the IT expenditure of the company against its competitors.

Are we spending efficiently on IT?

As computer technology and networks grow, spending efficiently on the IT infrastructure becomes more and more important. The cost of IT is not just the money spent on hardware and software. The **Total cost of ownership** must also incorporate the human (i.e. training) and maintenance aspects of running an IT system. Expenses which make up the total cost of ownership of an IT infrastructure include:

- **hardware** – the cost of purchasing equipment including computers, monitors, printers etc.
- **software** – the cost of purchasing or licensing software for each user
- **installation** – the cost of installing hardware and software
- **training** – the cost of providing training for both IT specialists and end users
- **support** – the cost of providing on-going technical support for employees and customers
- **maintenance** – the cost of repairing and upgrading hardware and software when necessary
- **infrastructure** – the cost of acquiring, maintaining and supporting related infrastructure such as networks, storage and other specialised equipment
- **downtime** – the cost to the company of loss of productivity caused by failure of any part of the IT infrastructure
- **space and energy** – the cost of housing and running all of the equipment that makes up the IT infrastructure.

Managers need to bear all of these costs in mind when deciding what IT infrastructure they should invest in for their organisation.

6.8 Summary

In this chapter we have seen that the evolution of technology has been fast and far reaching. We have come in the space of a few years from massive expensive mainframe computers to inexpensive, hand-held devices – and it is not stopping here. The seven major components of an IT infrastructure (hardware, operating system, software applications, data management and storage, networking/telecommunications, Internet platforms, consultancy and integration services) have to be merged to work as a cohesive system and the components have to keep up with new trends in technology and each other. We have looked at some of the reasons why technology is changing so much so quickly and we have discussed some of the newest hardware and software. We have seen what a difficult job it is for managers to keep their organisations in line with current trends without overspending on IT or causing meltdown amongst their employees by continually changing and upgrading their IT systems.

6.9 A reminder of your learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe the seven major components that make up an IT infrastructure;
- discuss the evolution of IT over the past 30 years since the first commercial use of mainstream computers to the present day;
- discuss the factors, including Moore's law and Metcalfe's law, that have driven the rapid evolution of technology;
- outline the emerging hardware trends including mobile devices, grid computing, cloud computing, autonomic computing, virtualisation and multi-core processors;

- outline the emerging software trends including Linux and other open-source software, Java, Ajax, Web service and applications;
- discuss the considerations that managers have to take into account when deciding upon an IT infrastructure for their organisation;
- describe the elements that make up the total cost of ownership of an IT infrastructure.

6.10 Chapter questions

1. Estimate the total cost of ownership of the technology in your own workplace or college. Do not forget to include each of the components listed in section 6.7.2 in your calculation.
2. Describe the five technology drivers of the IT infrastructure evolution. Which do you think has been the most influential?
3. Discuss how cloud computing can provide value to an organisation.
4. What is Java and how it is changing the computing environment?
5. Discuss the business value of open-source software.

Chapter 7

Managing information

7.1 Introduction

We have already seen in Chapter 1 that there is a difference between *data* and *information*. In this chapter we will look in more detail at how data can be stored and managed effectively to produce meaningful information. We will consider some of the problems that can occur with traditional data storage and management solutions and see how Database Management Systems (DBMS) can be used to minimise these problems and get the best out of stored data. We will see how data modelling is used to designed a database and that data policies need to be applied to ensure that the database is maintained correctly.

Essential reading

Laudon and Laudon, *Management Information Systems Managing the Digital Firm*, Chapter 6.

Additional reading

Turban and Volonino Technical Guide 3 from the student companion website for *Information Technology for Management*. This can be found at http://bcs.wiley.com/he-bcs/Books?action=resource&bcsId=4953&itemId=0470400323&resourceId=17218&chapterId=48688.

7.2 Learning outcomes

After studying this chapter and the recommended reading you should be able to:

- outline the benefits of having a centralised database which is accessible to all users and how database management systems can be used to help achieve this
- explain how information is stored on a computer and be familiar with the terms *bit, byte, field, record, file* and *attribute*
- discuss the terms *entity* and *attribute* and be able to suggest or identity appropriate entities and attributes in a given situation
- discuss the problems that can occur with traditional data storage solutions and explain how DBMS can overcome these problems;
- explain how a relational database stores data in tables and how these tables can be linked and merged to answer queries

- explain the importance of keeping a data dictionary which defines the data definition language used to specify the contents of the database
- discuss the terms *normalisation* and *entity relationship diagram* and explain how these techniques are used when data modelling prior to the construction of a new database
- discuss how using *data warehouses* and *data mining* can help companies improve their business
- explain the importance of having a *data management policy*.

7.3 Organising data

Data is an important business resource, but even though a company may compile millions of pieces of data, this does not mean that it can produce information that its customers, employees and suppliers can use. A competitive advantage can be gained by turning data into useful information.

7.3.1 Storing data on a computer

No matter how powerful it is, all a computer really stores is a string of 0's and 1's each of which is called a **bit**.

A string of eight bits is called a **byte**. One byte can be used to represent a character such as a letter, number or any miscellaneous character in ASCII. For example the ASCII code for the letter R is the byte 01010010.

By grouping together bytes, a computer can thus store names, numbers and so on. A group of bytes which represents a piece of information such as a name, is called a **field**.

A group of related fields form a **record**. For example the record *Student* maybe made up of the fields *firstname*, *surname*, *SRN*, *age*.

A group of records of the same type is called a **file**. Thus a file called *students_personal* would contain all of the student records for the students who are currently enrolled.

A group of related files is a **database**.

The hierarchy from bits and bytes up to files and databases is illustrated in figure 7.1.

Two other important terms are **entity** and **attribute**. An entity is the thing about which you are collating information. Thus an entity is likely to be a person, a place or an event. An attribute is a single piece of information about the entity. For example, in table 7.1 each column of the table describes an attribute (in this case firstname, surname, SRN, age, house_no, street, city, postcode, country), each row is for a different entity (in this case the two students RACHEL BASSETT and FRED FLINTSTONE).

bit: 0

byte: 01010010

field: *firstname*=RACHEL

record: *student*=

firstname	surname	SRN	age
RACHEL	BASSETT	079011010	24

file: *students_personal*=

firstname	surname	SRN	age
RACHEL	BASSETT	079011010	24
ElIZA	DOLITTLE	089328023	28
FRED	FLINTSTONE	074837283	45

database: student_personal_file
student_financial_file
student_marks_file
student_courses_file

Figure 7.1: bit→byte→field→record→file→database

←—attributes—→

firstname	surname	SRN	age	house_no	street	city	postcode	country
RACHEL	BASSETT	079011010	24	96	The Avenue	York	YO7 3RW	UK
FRED	FLINTSTONE	074837283	45	32	Rockville	Stones	12345	USA

Table 7.1: Entities and attributes

Learning activity

Suppose that you decide to create a database for a newspaper delivery business. You need to keep accurate information on all of your customers. You create a record for each customer.

- What attributes do you need for each customer?
- What are the entities in this case?
- Give an example *field*, *record* and *file* from the database.
- What other files might you need in this database?

7.3.2 Problems with traditional data storage

In chapter 2 we discussed the problems caused by different departments in an organisation not sharing their information with each other and thus making *islands of information*. This is often caused by different departments in a company each setting up their own file system. As figure 6.2 on page 238 of Laudon and Laudon shows, in a traditional set-up, the accounting and finance, human resources, sales and marketing and manufacturing departments all use separate applications. These applications require data from the master data file. Often the different departments

will require the same data – for example accounting and finance and human resources will both need to have access to all the employees' personal details such as full name, address, date of birth, etc. If the two different departments each keep their own records of this information this is not only inefficient but can lead to problems including data redundancy and inconsistency, program-data dependence, lack of flexibility, poor security, lack of data share and availability. We will describe each of these problems in turn.

- **Data redundancy** occurs when the same piece of information is entered into the same database twice. Perhaps there is one file called customer_details and another called enquirer_details. If you first registered with a company, for example on a website, but did not buy any goods, your details may have been stored in the enquirer_details file. If at a later date you bought something from the company, then your details may also have been added to the customer_details file. This is data redundancy. If the company sends out Christmas cards, it is likely that you will get two – not because you are particularly popular but because you occur as two different entities in the database. Furthermore, if you later move house and inform the company of your new address, it may be updated in the customer_details file but not in the enquirer_details file. Next Christmas you will get a card at your new address and a second one sent to your old address. This is **data inconsistency** – the same entity has different attributes according to the database.

- **Program-data dependence** occurs because some computer software programs, in particular those written for large mainframes, require data to be constructed in a particular way. Data that is constructed for one program cannot be used in another which requires a different configuration. If a company wants to use the same data in a different program, it will have to reconstruct it accordingly. It is a waste of time and money to have to maintain the same data in different formats due to program-data dependence.

- **Lack of flexibility** can occur if different people require different information from the same entities. For example, the Sales and Marketing department might need information about the company's new production schedule, but they do not need as much detail as the Production department, and their priorities are different so they would like the information presented in a different order. Traditional file systems may not be able to oblige – the Sales and Marketing department will have to put up with the data in whatever format it appears.

- **Poor security** can be a problem as traditional file environments typically have little or no security controls over who has access to what data. In the modern world where data control and data privacy are often legal requirements, this is unacceptable. Furthermore, if data is held in several separate file systems, then all of these need to be secure.

- **Lack of data share and availability** can occur if someone wants information about something and the attributes are stored in different databases in different departments. Suppose for example that the Chief Executive wants to compare the sales of Part A with the production schedule for Part A. If the attributes regarding production are held in one file system in one format in the Production department, and the attributes regarding sales are held in another file system in a different format in the Sales department then it could be hard for the Chief Executive to get the information they require in a usable format.

7.4 Databases

Database technology can be used to minimise many of the problems described above that can occur with traditional file storage. As we said before, a database is a group of related files. This is a basic definition and does not take into account the fact that the database should be in some ordered and useful form. A better definition is as follows.

> A **database** is a collection of data which is organised so as to be able to serve many applications efficiently.

In an effective database this is done by centralising the data and removing data redundancy. Instead of storing separate files for each application, the data is stored in one location and used by each of the separate applications. This can be achieved by using a database management system or DBMS.

7.4.1 Database management systems

A **database management system (DBMS)** is basically a piece of software that enables a company to centralise its data, manage it effectively and provide access to the stored data by application programs. The DBMS removes the onus from the data user to know where the information that they require is and what format it is in.

For example, if the company accountant is using an application that requires the gross pay for all employees then the DBMS will obtain this data from the database and present it to the application program in the correct format, without the accountant having to know exactly where, or in what format, that data is stored in the database.

In general, the end users of the database are unaware of what the database looks like, where anything is stored and how the information is organised. To someone working in Personnel, it might seem that the logical way to store employee records is in alphabetical order by name. In actual fact, the employee records are probably stored in the database ordered by a unique identifying number. However, if the Personnel department request a list of employees in alphabetical order from the database then this is what the DBMS will deliver.

Figure 7.2 shows that two different departments (Academic and Finance) can get different views of the data held in the Student database.

The benefits of using a DBMS

Using a DBMS can solve or minimise some of the traditional problems described in section 7.3.2 associated with data storage in a large organisation.

- There is just one database serving the entire organisation. This eliminates the problem of having **islands of information** with one department having information which others do not have access to.
- There should be only one instance of each entity in the database. This eliminates

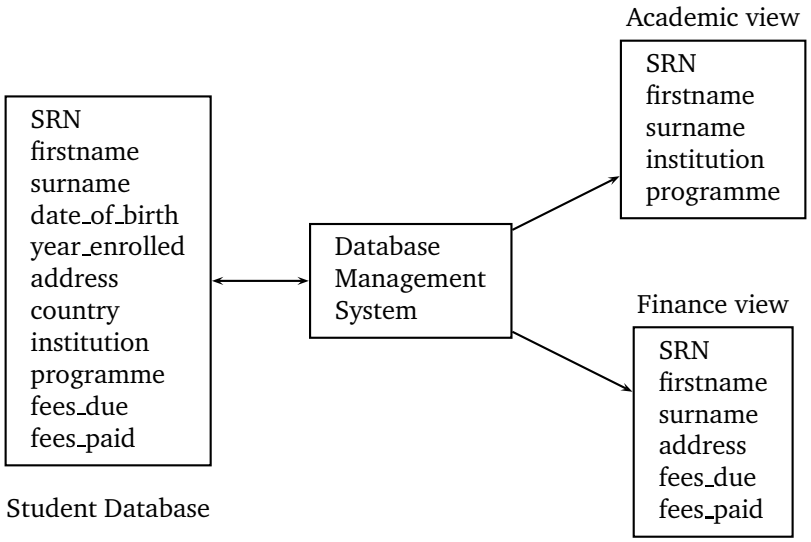


Figure 7.2: Different departments can get different views of data from the same database using DBMS

the problem of **data redundancy**, and reduces the problem of **data inconsistency** – when changes occur only one record needs to be updated and thus it is much easier to maintain information that is correct, consistent and up to date.

- The data is constructed in the centralised database separately from the programs that will use it. The DBMS arranges the data into the correct format for the application that is requesting it at the time of the request. This eliminates the problem of **program data dependence**.
- The problems of **lack of flexibility** and **lack of data share and availability** are resolved as the DBMS can present whatever data is required by whichever application in the appropriate format. Now the Chief Executive can request data on sales and production and these can be delivered in a usable format. The Sales and Marketing department can get information about the new production schedule without being bogged down in details that they do not require.
- It is much easier to secure and provide access control for one centralised database than it is to control access to multiple databases or file systems. Thus the problem of **lack of security** is minimised (although proper security and access controls still need to be maintained – see Chapter 9).

7.4.2 Relational databases

A **relational database** stores data in tables. The data is then extracted and merged into whatever format the user (or application) requires. The tables are sometimes referred to as files but this is confusing since it is possible to have multiple tables within a file.

The data in each table is broken down into **fields**. Each column of the table

represents a field and contains a single attribute[1].

A group of fields (a row in the table) is a **record**.

Table 7.2 is an example of a relational database table. Each column represents a field and contains a single attribute. Each row holds a record.

firstname	surname	**SRN** (key field)	age	house_no & street	city	postcode	country
RACHEL	BASSETT	**079011010**	24	96 The Avenue	York	YO7 3RW	UK
FRED	FLINTSTONE	**074837283**	45	32 Rockville	Stones	12345	USA

Table 7.2: A relational database table

Each table in a relational database must have a **key field** which is a field of unique identifiers. In table 7.2 the key field is the SRN (student registration number). This is a number that is unique to the student and does not change throughout their enrolment with the University. There could be two students called FRED FLINTSTONE but each will have a unique SRN and this can be used to distinguish between the two students. In other instances, the key field might be your social security or national insurance number or your house number combined with your postcode and initials.

The key field contains the **primary key** for each record. When tables are used in relation to each other, the primary key from one table is stored as the foreign key in the other and vice versa. In this way the two tables have a direct relationship. For example, consider the simplified *Customer* and *Order* tables in figure 7.3.

Customer Table

Customer_Name	Customer_Address	**Primary Key Customer_ID**
Joe Bloggs	27 West Street	**JB27090427**

Order Table

Primary Key Order_Number	Order_Item	Quantity
78642193	blue jeans	2

Figure 7.3: Simple tables with primary keys in a relational database

Details about orders are not stored in the customer table and details about customers are not stored in the order table. It is important that only attributes for a particular entity are stored with that entity. However it is also important that the order that Joe Bloggs placed can be tracked and related to him. The Order_Number which is the primary key in the Order Table is stored as the foreign key in the Customer Table. Likewise the Customer_ID which is the primary key in the Customer Table is stored as the foreign key in the Order Table. This is shown in figure 7.4.

Now starting with the Customer ID we can look Joe Bloggs up in the Customer Table and find the Order Number which is stored there as the foreign key. Now we can use the Order Number to look up the relevant order in the Order Table. The foreign key in the Order Table is that of Joe Bloggs Customer ID so we know that we are looking

[1]Note that the smallest possible fields should be used for each record. For example it is much better to have separate attributes for *firstname* and *surname* rather than a single attribute for *name*. This makes it much easier to sort and manipulate the records.

Customer Table

Customer_Name	Customer_Address	**Primary Key Customer_ID**	**Foreign Key Order_Number**
Joe Bloggs	27 West Street	**JB27090427**	**78642193**

Order Table

Primary Key Order_Number	Order_Item	Quantity	**Foreign Key Customer_ID**
78642193	blue jeans	2	**JB27090427**

Figure 7.4: Simple tables with primary and foreign keys in a relational database

at the correct record.

Similarly we could start with an Order Number and find out details about the customer who placed the order by using the Customer Number that is stored as the foreign key in the Order Table and looking it up in the Customer Table.

Operations used to manipulate a relational database

Any two tables in a relational database can be combined so long as they share a common data element. There are three basic operations.

- **Select** – create a subset of records that meet your criteria.
- **Join** – combine related tables to provide more information than is available in an individual table.
- **Project** – create a new table from subsets of previous tables.

Using these operations it is possible to manipulate the data available in all of the different database tables to provide whatever information is requested in the desired format.

Figure 6.5 on page 244 of Laudon and Laudon illustrates how these operations are used to combine information from the PART table and the SUPPLIER table to construct a new table with only specified attributes about suppliers for particular parts. First the relevant parts are **selected** by Part_number from the PART table. The two tables have a common data element, namely Supplier_Number. This information is used to **join** the two tables so that information about the suppliers for the relevant parts is captured. Finally the data is **projected** into a new table showing only the parts and information about the suppliers that are of interest for this particular query.

7.4.3 Tools that a DBMS should provide

A DBMS should provide tools for organising, managing and accessing the data in the database. These include:

- **A data definition language** which is used to specify the contents of the database. This is required to create database tables and to define the

characteristics of the fields in each table. This makes sure that all users of the database are 'talking the same language'.

- **A data dictionary** is used to store each data definition in the data definition language. For each data element or field in the database the characteristics of that element should be stored in the data dictionary, and this should be available to all users. This is especially important in case the person or people who initially designed the database move on – what might have been obvious to them might not be so to the next database programmer. Users and programmers can also consult the data dictionary to check what data elements are already available before creating unnecessary new ones. This can help to eliminate data redundancy and inconsistency.
- **A data manipulation language** is a formal language used to manipulate the data in the database and make sure that it is formatted and presented as useful information. The language should make it easy for users to build their own queries and reports. **SQL (Structured Query Language)** is the most well-known data manipulation language and is now embedded in some desktop applications such as *Microsoft Access*.

7.5 Designing a database

7.5.1 Data modelling

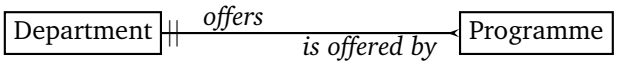
Before creating a database, it is important that you think hard about the information it is going to be used for and how the different parts of that information are related to each other. How should the information be stored, organised and used? Data modelling is the process of defining the data that is going to be used or produced within an information system and how it is organised. The basic tool used for data modelling is an **Entity Relationship Diagram**

Entity Relationship Diagrams

An entity relationship diagram (ERD) is a technique used to identify the entity types in a particular situation and diagram the relationships between them. Figure 7.5 shows an entity relationship diagram for part of a university registration system. The diagram identifies five entity types (Department, Course, Professor, Programme and Student) and the relationships between them.

The symbols, $||$, $<$ and $o<$ used on the relationship lines signify whether the relationship is one-to-one, many-to-one, or many-to-many. A $||$ symbol signifies a -to-one relationship. A $<$ or $>$ symbol signifies a -to-many relationship. A $o<$ or $>o$ symbol signifies that there may be zero, one or more.

For example the relationship between Department and Programme is one-to-many. The Department offers many programmes, but each programme is only offered by one department.



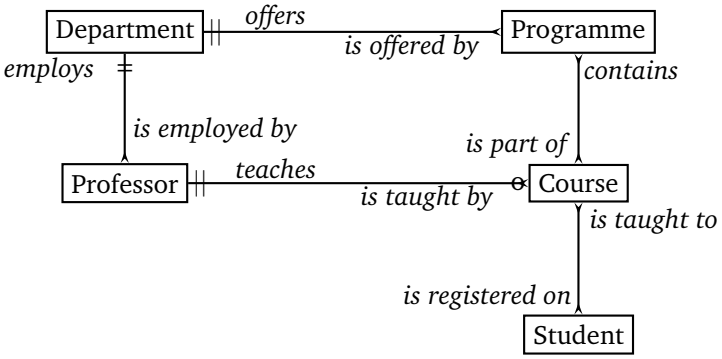


Figure 7.5: An ERD for part of a university registration system

Similarly, each Professor is employed by only one Department, but each Department employs many Professors.

A Professor may teach zero or more Courses, but each Course is taught by only one Professor.

A Course is taught to many Students and many Students are registered on each Course.

A Course may be part of many Programmes and a Programme may contain many Courses.

Identifying the data in a database

After identifying the entity types and the relationships between them, the next step is to identify the data that should be in the system. For each entity, this data consists of the significant attributes. For example, the entity Course may have attributes course_number, department, professor, level, description. As the analysis of the system continues, these attributes might be re-named or modified and other attributes may be added. It is important to keep asking yourself the following questions until the answer to them all is "No".

- Is any data missing about each entity type?
- Is there any ambiguity in what the various attributes mean?
- Does the same attribute appear in two places?

Analysing the data to be included in a database requires a great deal of thought and attention to detail. Several versions of the set of entity types, attributes and relationships may need to be produced.

Learning activity

Consider the entity relationship diagram shown in Figure 7.5.

1. Add a new entity called *University* given that the University has many Departments but each Department belongs to only one University.

2. For each of the entity types in Figure 7.5 list the attributes that you think should be stored for that entity.

Normalisation

It is important to avoid redundancy between tables and not to allow a relationship to contain repeating data groups. For example do not allow two tables both to store a customer's name. That makes it hard to keep data properly organised and updated. Minimising redundancy and increasing the stability and flexibility of databases by reducing data in the tables to its simplest form is called **normalisation**.

See figures 6.9 and 6.10 on pages 247 and 248 of Laudon and Laudon for an example of the normalisation process.

Referential integrity

Referential integrity rules should be applied to relational database systems to ensure that the relationship remains consistent. This means that if you create a table that points to another table, you can only add a new record to one of the tables if you also add a corresponding record to the second table. For example, consider the Customer and Order tables of figure 7.4. If we want to add a new order to the Order Table then we must also add a corresponding Customer to the Customer Table (assuming that this customer does not already exist in the customer table). Similarly, we cannot add a new customer in the Customer Table without adding a corresponding order in the Order Table. This is shown in figure 7.6

Customer Table

Customer_Name	Customer_Address	**Primary Key Customer_ID**	**Foreign Key Order_Number**
Joe Bloggs	27 West Street	**JB27090427**	**78642193**
David Cameron	10 Downing Street	**DC10141138**	**78642194**

Order Table

Primary Key Order_Number	Order_Item	Quantity	**Foreign Key Customer_ID**
78642193	blue jeans	2	**JB27090427**
78642194	blue tie	1	**DC10141138**

Figure 7.6: Adding corresponding records in related tables

7.5.2 Distributed databases

When designing a database, it is also important to consider how the data is to be distributed. Information systems can be designed with a centralised database that is used by a single central processor or by multiple processors in a client/server network. However, in very large organisations that require immediate fast access to data at multiple sites a **distributed database** will be required. There are two ways to structure a distributed database.

- **Partition the database** – some parts of the database are stored and maintained at one location and other parts are stored and maintained at other locations. Each remote processor has the data that it needs to serve its local area. Changes to the local databases are implemented on a central database at regular intervals, for example every night.
- **Replicate the database** – the entire central database can be duplicated at all the required remote locations. Generally changes made to the *master* database are also made in the duplicate versions. As with a partitioned database these changes would be made automatically at regular intervals such as every night.

Learning activity

Discuss the advantages and disadvantages of using:

1. A distributed database rather than a centralised database.
2. A partitioned database rather than a replicated database.

7.6 Improving business using databases

Companies and organisations use databases to keep track of day-to-day transactions such as paying employees and suppliers, processing orders, storing customer information, keeping an inventory of stock and so on. However, databases can also be used to provide information that will help the company run more smoothly and get (or keep) its competitive advantage. In a large company, special tools are needed to be able to effectively analyse the vast amounts of data that is stored. These tools include data warehousing, data mining, and application servers that enable the access of databases through the Internet. We will look at each of these in turn.

7.6.1 Data warehouses

A data warehouse is basically a set of huge computer files that store old and new data about everything that a company wants to maintain information on. The data may come from different information systems throughout the company and as such may be in different formats. The data warehouse uses software to consolidate and standardise the information that is gathered so that it can be used across the entire organisation for management analysis and decision making.

The process of creating and maintaining a data warehouse involves the following steps.

- **Extraction** – regularly downloading new data from different internal data sources (for example Manufacturing Data and Customer Data) and external data sources.
- **Consolidation** – combining the data from the different data sources.
- **Filtering** – removing any data that is not needed for analysis purposes.
- **Cleansing** – identifying any errors or duplications and correcting them.
- **Transformation** – modifying the data so that it is consistent with the data definition language.
- **Aggregation** – summarising the data for analysis.
- **Updating** – keeping the data warehouse up to date by adding new data.

The data in the data warehouse should be widely available across the organisation, but it cannot be altered by people using the information. Many companies use an Intranet portal to give their employees access to the data warehouse information. An information directory provides users with information about the data available in the data warehouse. Query tools, analytical tools and graphical reporting tools are used to enable users to get the information that they require in a useful format.

Learning activity

The case study on pages 252-253 of Laudon and Laudon describes how the American Internal Revenue Service is using a data warehouse to improve its ability to manage and make use of the data it has collected. As a result the agency has recovered many billions of dollars in tax revenue that was lost under the old system.

Read the case study and answer the questions on page 253.

Data marts

A data warehouse can be daunting because of its size and the huge amounts of data it stores. A company can break the information down into smaller groups called *data marts*. These are generally focused on a particular subject or line of business such as Sales and Marketing. It is easier and cheaper to sort through a data mart than the entire data warehouse.

7.6.2 Data mining

Organisations collect millions of pieces of data. Using the right tools, the organisation can use this data to develop effective competitive advantages as discussed in previous chapters. Instead of guessing about which products or services are the best sellers, **business intelligence tools** which consolidate, analyse and provide access to data, provide concrete methods for analysing exactly what customers want and how to supply it to them.

Online analytical processing (OLAP) supports multidimensional data analysis, enabling users to view the same information in different ways. A good analogy is a Rubiks Cube. The six coloured faces represent six different aspects of information –

sales, pricing, cost, region, period and product for example. The cube can be jumbled up so that different faces are adjacent. Thus any aspects can be compared with each other – rearranging the cube gives a different view.

Three benefits of using business intelligence tools include:

- the capability to amass information
- the development of knowledge about customers, competitors and internal operations
- the ability to change decision-making behaviour to achieve higher profits.

Data mining goes one step further than Business Intelligence or OLAP tools. Data mining technology attempts to find hidden patterns and relationships in large databases and hence predict future behaviour. The types of information which can be obtained by data mining include:

- **associations** – determining which occurrences are linked to a single event
- **sequences** – determining which events are linked over a period of time
- **classifications** – discovering characteristics of customers and making predictions about their behaviour
- **clustering** – discovering groups within data
- **forecasting** – using existing values to forecast what other values will be.

Learning activity

One problem with data mining is that it can produce information that seems useful but actually is not meaningful in the context of the company. For example, suppose that data mining tells a retail company that on a hot summer's day more bottled water is sold in convenience stores rather than in supermarkets. Data mining also reveals that when customers purchased white socks they also purchased bottled water 60% of the time and when they purchased black socks they also purchased bottled water 57% of the time.

Which pieces of information do you think are useful when the company is making decisions about where to send its stocks of bottled water and socks?

Text mining and **web mining** tools are also available. These can be used to discover patterns and relationships from text documents and web pages.

7.6.3 Databases and the Internet

Web browsers are generally much easier to use than query languages. It is often easier for companies to provide their employees, customers and suppliers with web-based access to their database(s) rather than creating proprietary systems. It is also cheaper to create *front end* browser applications that can link information from different systems rather than trying to combine all of the systems at the *back end*. Internal databases can be linked to the web using software programmes that provide a connection to the database without the need for a major reconfiguration. A **database server** is a special dedicated computer that maintains the DBMS. A software program called an **application server** processes the transactions and offers data access. A user making an enquiry through the web server can connect to the company's database and receive information in the form of a web page.

The benefits of using a web browser to access a database include:

- ease of use
- less training required for users
- no changes required to the internal database
- the company can keep its old legacy system instead of having to replace it
- cheaper than building a new system
- creates new efficiencies and opportunities
- provides employees with an integrated company-wide view of information.

7.7 Data management policies

Setting up the company database is only the beginning. In order to ensure that the database remains accurate, reliable and accessible, the company will need to establish policies and procedures for data management.

No single part of the organisation should feel that it has exclusive ownership of any of the information in the database. Although a particular department may have the responsibility for updating and maintaining the data, or part of the data, that department still has to share the information across the whole organisation. An **information policy** should be written which outlines rules which govern how the information in the database will be shared, maintained, distributed and updated.

Someone (possibly a whole team of people) needs to be responsible for **data administration**. They will be responsible for:

- developing information policies
- planning for data
- overseeing logical database design
- developing the data dictionary
- monitoring use of data.

Data governance is concerned with the policies that govern the security, integrity, privacy and access controls of the information.

7.7.1 Data quality

If a database and information policy is properly designed then the company should be able to gather the information that it requires. Furthermore duplications and inconsistent data should be minimal. However, it is still important that data quality is maintained. Errors in the database should be identified and corrected. This can be done using a **data quality audit** which might:

- survey the files of the entire database
- survey a sample of files from the database
- survey end users about their perceptions of the data quality.

If data quality is poor than the information obtained from that data will also be of poor quality.

7.8 Summary

In this chapter we have looked at ways of turning data into information. We have seen how the problem of creating islands of information within an organisation can be avoided by having a centralised database which is accessible by everyone. We have seen how database management systems can be used to help organisations get the most benefit from their database. We have discussed relational databases and how separate tables of information can be merged so that queries regarding different aspects of a product for example can be answered. We have seen how data modelling and entity relationship diagrams are used to help design an effective and efficient database. We have considered the problem of distributed databases and discussed partitioning and replicating the central database as possible solutions. We have seen how data warehouses, data mining techniques and the Internet can be used to help organisations use the data that they have gathered to improve their competitive advantage. Finally we have discussed data management policies and seen that an information policy is necessary in order for the database to be correctly used and maintained.

7.9 A reminder of your learning outcomes

After studying this chapter and the recommended reading you should be able to:

- outline the benefits of having a centralised database which is accessible to all users and how database management systems can be used to help achieve this;
- explain how information is stored on a computer and be familiar with the terms *bit, byte, field, record, file* and *attribute*;
- discuss the terms *entity* and *attribute* and be able to suggest or identity appropriate entities and attributes in a given situation;
- discuss the problems that can occur with traditional data storage solutions and explain how DBMS can overcome these problems;
- explain how a relational database stores data in tables and how these tables can be linked and merged to answer queries;
- explain the importance of keeping a data dictionary which defines the data definition language used to specify the contents of the database;
- discuss the terms *normalisation* and *entity relationship diagram* and explain how these techniques are used when data modelling prior to the construction of a new database.
- discuss how using *data warehouses* and *data mining* can help companies improve their business;
- explain the importance of having a *data management policy*.

7.10 Chapter questions

1. What are the problems associated with managing data in a traditional file environment and how can they be resolved by using a database management system?

2. Describe how a relational DBMS works and explain why it is a powerful tool in terms of turning data into information.
3. What do you think are the benefits of using a web-like browser to access information from a database?
4. To what extent do you think that end-users should be involved in the selection of a database management system and database design?
5. Describe three technologies or tools that can be used to access information from databases to improve business performance and decision-making.

Chapter 8

Telecommunications

8.1 Introduction

In this chapter, we will describe the role that networks and telecommunications play in an e-commerce business. We will see how traditionally separate computing and communications systems are merging into universal systems which perform both functions. We will describe the layout of different networks for use in personal and business settings. We will examine the different components of a telecommunications network and describe how they are used to generate, transmit and receive data. Finally, we will look at the biggest network of all – the Internet.

Essential reading

Laudon and Laudon, *Management Information Systems Managing the Digital Firm*, Chapter 7.

Additional reading

Turban and Volonino Technical Guide 4 from the student companion website for *Information Technology for Management*. This can be found at http://bcs.wiley.com/he-bcs/Books?action=resource&bcsId=4953&itemId=0470400323&resourceId=17218&chapterId=48688.

Grulke, Wolfgang E, *"In Search of Simplicity" (Beyond the Search for Excellence) Information Management Tools: Their Future and Their Potential Impact on the Corporation.* This paper can be found at www.futureworld.ord/Archives/tlksimpl.html Find out how Google works at *http://www.googleguide.com/google_works.html*

8.2 Learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe how telecommunications technology has evolved over the past 20 years
- describe the component parts of a computer network and draw a simple local area network (LAN)
- describe a LAN in terms of its topology and discuss the advantages and disadvantages of different topologies
- describe the three computer network technologies client/server computing, packet switching and TCP/IP and understand how important these technologies are in enabling the development of telecommunications

- explain the difference between digital and analogue signals and why a modem is necessary to transfer between the two different types of signal
- describe the different types of communication channels that can be used for a wired network and discuss the advantages and disadvantages of each
- describe the different types of communication channels that can be used for wireless networks and discuss the advantages and disadvantages of each
- understand that the Internet is an example of a wide area network (WAN) and describe briefly how the Internet works and the services that it offers including the web.

8.3 Evolution of telecommunications

Telecommunications is the transmission of data between computing devices on a network. Such computing devices may be desktop computers, laptops, mobile phones, blackberries etc. *Data* comes in many forms and might be spoken, written, pictorial, video and so on.

Until recently, different types of data were transmitted by different networks each operated by a different service provider. For example, in Britain twenty years ago if you wanted to speak to someone you would use the telephone and this service would be provided by the telephone company British Telecom. If you wanted to write to someone, you would post a letter using the Royal Mail. If you wanted to watch television you would pay your TV licence and watch BBC1, BBC2 or ITV. To send an email you would connect your computer to your telephone line (thereby making it unavailable for telephone calls) and download rates were very slow. Gradually these services started to merge and new service providers such as Sky and Virgin came into the picture. Now it is possible to buy a *package of services* all from one provider and this will include your fixed line phone, mobile phone, satellite or cable television, and broadband Internet access.

In his paper *In Search of Simplicity* published in 1987, Wolfgang Grulke made the following predictions regarding the future of telecommunications:

> *Telecommunications standards and architectures are beginning to be much more consistent across these types of data and increasingly across different vendors. Both vendor-initiated architectures (such as IBMs Systems Network Architecture, and the equivalent office information architectures) and industry initiatives such as open systems interconnect are seeing to that.*
>
> *It is now possible to connect personal computers to a wide variety of information networks and data bases. Financial institutions are co-operating in sharing networks and automated teller machines. "We owe it to the future to begin to get ready now."*
>
> *All these initiatives make any given computer much more powerful and useful, and a far better return on investment. That can only lead to new phenomenal growth in the long-term, which will continue to be fuelled by a host of new possibilities, some as yet unseen. Already the electronics revolution has started the convergence of the publishing, broadcasting and entertainment industries.*

Grulke was right. The publishing, broadcasting and entertainment industries have indeed merged and as high-speed broadband network connections continue to expand and service providers continue to develop products it is becoming harder to

tell where one ends and the next begins. Gradually computers are becoming communication devices and communication devices are becoming computers.

Learning activity

Twenty or so years ago Grulke predicted where we would be now in terms of telecommunications. Where do you think we will be in another 20 years' time?

8.4 Computer networks

Any two or more computers which are connected form a *computer network*. Figure 8.1 shows the components used in a simple network structure. These include:

- client computers
- a dedicated server computer
- a hub or switch
- a network operating system (NOS)
- network interface cards (NIC).

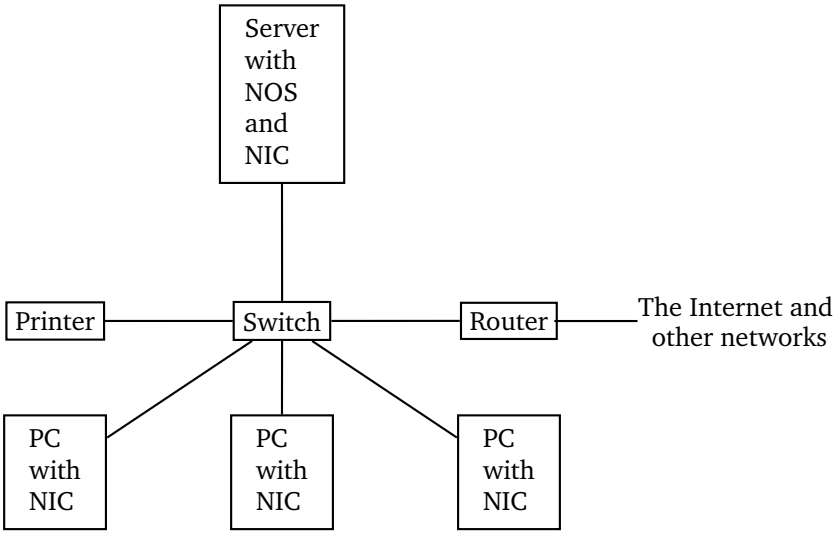


Figure 8.1: A simple client/server LAN

It is possible to keep on adding components to this type of network and expand it to meet requirements. By putting a *Network Interface Card (NIC)* into a personal computer (most PCs have a built in NIC these days) you can incorporate it into an existing network. To share network resources such as printers, you need special software called an *Network Operating System (NOS)*. The NOS might be installed on

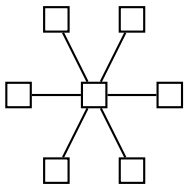
every computer in the system, or it might be on a dedicated server. In this case the server computer performs network functions for the client computers such as delivering web pages and storing data. Examples of the most widely used Network Operating Systems are *Microsoft Windows Server, Linux* and *Novell Netware*. *Hubs* and *switches* are used to help route traffic on the network to the right computing device. If you want to communicate with another network such as the Internet then you also need a *router* which is a communication processor used to ensure that data transmissions get sent to the correct address. A very large network may require multiple routers to make transmissions flow more quickly.

8.4.1 LANs and WANs

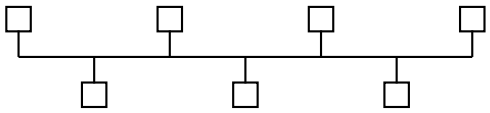
The computer network described above is a *Local Area Network (LAN)* which connects personal computers and other devices in a local area such as an office floor or a building. This is suitable for small company. The LAN shown in figure 8.1 is an example of a client/server architecture with the network operating system residing on a single file server. Alternatively, the LAN may have a *peer-to-peer* architecture whereby all the computers are treated equally (there is no dedicated server computer in a peer-to-peer network).

LANs may be described in terms of their *topology* – the way in which they are connected together. Examples of LAN topologies are star, bus and ring, mesh and hierarchical.

- **Star** – in a star topology all of the devices are connected to a single hub through which flows all network traffic.

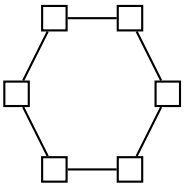


- **Bus** – in a bus topology there is a single transmission segment along which all messages are sent in both directions. All of the machines on the network receive the same signals, but each client computer has software installed which allows it to listen out for messages addressed to it. The bus topology is the most common *Ethernet*[1] topology.

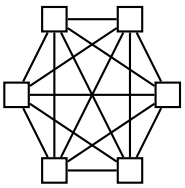


- **Ring** – in a ring topology the network components are connected in a closed loop. Messages pass from one computer to the next moving in one direction only around the loop. Typically only older LANs use a ring topology.

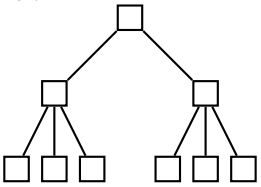
[1]Ethernet is a standard computer networking technology for LANs. It defines wiring and signalling standards formalised as IEEE 802.3



- **Mesh** – in a mesh topology every component is connected to every other component. The advantage of this is that if one component fails the rest of the network is not effected. The disadvantage is the cost of installing all of the connections and the relative difficulty of adding a new component to the network since it has to be connected to every other component.



- **Hierarchical** – in a hierarchical network the components are arranged like an upside-down tree with the root being the mainframe computer at the top level and the leaves being the computer terminals at the bottom level. This type of network is relatively inexpensive to set up, and it is easy to scale the size of the network up and down. A disadvantage is that traffic jams can occur at the top level.



Learning activity

Suppose that you are asked to design a local area network (LAN) for a public library. There will be eight computers which library customers can use to log onto the Internet, search the library records and print using a single printer. What equipment would the library need and what topology would you recommend for this LAN and why? Draw a diagram of your proposed LAN.

The network for a large company with employees in many different locations is not that different. It is a collection of many LANs connected together in a company-wide infrastructure. There are more computing devices and servers, but the basic network infrastructure is the same as for a LAN. This type of network is called a *Wide Area Network (WAN)*.

The Internet is an example of a WAN that connects many personal computers to Internet service providers (ISP) who in turn are connected to form a network. Once a user connects their PC to their ISP, a connection is made to a *name server* so that the content requested by the user can be retrieved. The name server will contain a list describing how and where to find this content. Requests are then made for this content and these are routed to the web server that contains them.

8.4.2 Computer network technologies

Three key technologies form the basis of modern computer networks and the Internet. These are client/server computing, packet switching and TCP/IP. We will look at each of these in turn.

Client/server computing

We talked about client/server networks in section 6.4. Instead of having a huge mainframe with user terminals, many companies now use a client/server network with each client computer being a powerful (although relatively inexpensive due to Moore's Law) piece of equipment in its own right. All of these client computers are linked together in a network that is controlled by the network server computer(s). This type of network is ideal for a company that is continually adding to and upgrading its hardware.

Packet switching

Before packet switching technology was developed communications channels such as telephone lines had to be dedicated to a particular job (connecting two remote LANs for example) and remained unused at periods when no data was being sent. This was an expensive and wasteful use of resources. With the development of packet switching, much more efficient use is made of the communication channels available.

In packet switching, the data to be transmitted is split up into small chucks called *packets*. Each packet includes details about the address the packet is going to and transmission error checking information. Each packet travels independently over the network, being directed by the routers over the most efficient and economical available route. When they arrive at their destination, having travelled over many different routes through the network, the packets will be checked for transmission errors and reassembled into the original message. This all happens so quickly that you would not know that the message/web page/music download etc. has been split up and reassembled between leaving its source and arriving at your computer.

TCP/IP

In a telecommunications network, different hardware and software components need to work together. Fortunately, these different components can communicate with each other easily due to the *Transmission Control Protocol* and *Internet Protocol (TCP/IP)*. These protocols are a set of rules and procedures which govern how information is to be transmitted between two points in a network. We said in Chapter 6 that one of the driving factors in the increase and evolution of IT infrastructure is the existence of protocols which mean that components work together. I can sit in the UK and request a web page that might be stored on a server on the other side of the world safe in the knowledge that my computer, the computer storing the page I am requesting, and all of the computers in-between that link us, whatever hardware and software they comprise, can all communicate together using the same language.

TCP handles the movement of data between computers and IP is responsible for the delivery, reassembly and acknowledgement of packets. TCP/IP was originally created for the Internet, but it is easily transferred to networks of all sizes. Using TCP/IP models, companies can create web-based interfaces for different databases, for data input/output and for accessing information without having to physically combine all of the data in one huge computer.

There are four layers in the TCP/IP reference model for communication.

- **Application** – the application layer enables the client computer to access the other layers. It defines the protocols that applications use to exchange data such as the Hypertext Transfer Protocol (HTTP) which is used to transfer web pages.
- **Transport** – the transport layer provides the application layer with communication and packet services including TCP.
- **Internet** – the Internet layer addresses, routes and packages the data packets called IP data-grams using protocols including IP.
- **Network interface** – the network interface layer places packets on, and receives packets from, any networked technology.

Data sent from one computer to another passes down through the four layers:

Application → Transport → Internet → Network interface

and is then reassembled at the recipient computer by passing up through the four levels:

Network interface → Internet → Transport → Application.

8.5 Telecommunication media

A computer only understands *digital signals*, that are basically a stream of bits (1s and 0s represented by an electrical pulse being *on* and *off* respectively). However most data in a network is transmitted over telephone lines, and these lines only understand *analogue signals* which are continuous waveforms. In order to change the signals between digital and analogue you need a *modem* as shown in figure 8.2.

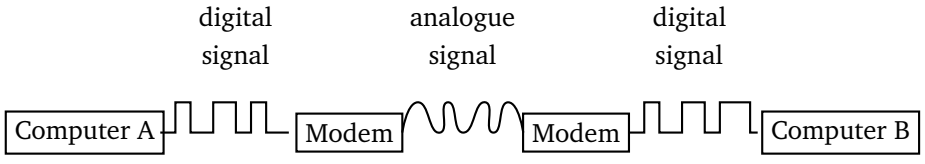


Figure 8.2: A modem converts digital to analogue signals and vice versa

A modem (short for modulator-demodulator) is a communications device that translates digital signals from a computer into an analogue signal that can be transmitted over a telephone line. The modem also translates analogue signals that have been transmitted over a telephone line back into a digital signal that the computer can understand. Most computers have built in modems these days.

8.5.1 Wired networks

A wired networks can use different kinds of physical wires and cables to transmit data. These include:

- **Twisted wire** – strands of copper wire twisted together in pairs in order to reduce the effect of electrical noise. Many buildings already have twisted wire installed for their telephone systems and these can be used for digital communication as well.

- **Coaxial cable** – insulated copper wire surrounded by a metallic shield and wrapped in a plastic cover. Coaxial cable is much less susceptible to interference than twisted wire and can carry a much greater amount of data. However it costs more and is less flexible than twisted wire, making it more expensive to install. Data transmission over coaxial cable can be divided into two types – Baseband and Broadband.

  - **Baseband transmission** is analogue with each wire carrying only one signal at a time.

  - **Broadband transmission** is digital with each wire carrying multiple signals at the same time. This makes broadband faster and better for high volume use than baseband transmission and hence broadband is currently the most popular choice for Internet access.

- **Fibre-optic cable** – strands of clear glass fibre though which pulses of light (instead of electronic pulses) are transmitted. Fibre-optic cables are gradually being used to replace copper cables as they are much faster and have a larger bandwidth. They can also carry signals for a longer distance and are cheaper to maintain than copper cables. They are ideal for high definition television broadcasts due to their high bandwidth.

The advantages and disadvantages of these three types of wired channel are summarised in table 8.1.

Type of channel	Advantages	Disadvantages
Twisted wire	Inexpensive Already in place Flexible	Relatively slow Low bandwidth Subject to interference (both electrical and) *phone tapping*)
Coaxial cable	Faster than twisted pair Higher bandwidth Less subject to interference	More expensive Less flexible
Fibre-optic cable	Very high bandwidth Relatively inexpensive Hard to *tap* i.e. more secure	Hard to work with

Table 8.1: The advantages and disadvantages of wired communications media

8.5.2 Wireless networks

The alternative to wired networks is *wireless communications*. Wireless communication devices, including mobile phones, communication satellites, wireless broadband, personal digital assistants (PDAs) and so on, are becoming increasingly popular.

Wireless communication is based on radio signals of various frequencies and can make use of microwave signals, satellites, radio signals, infrared signals and cellular radio technology.

- **Microwave systems** transmit high frequency radio signals at the speed of light. The signals only travel in a straight line and so they must be *bounced* around corners (such as around the curve of the earth's surface) by relay stations placed approximately 35 miles apart. Microwaves can carry approximately 10 times the amount of data as a cable and a microwave transmission system can be set up much more quickly than covering the same distance with a cable transmission system.
- **Satellites** are space stations that receive microwave signals from Earth, amplify the signals and bounce them back over a wide area. The advantage of satellites is the huge coverage they provide. Although the microwaves can still only travel in a straight line, the satellite is so far above the earth that it can send the microwaves to a huge area. For example, a network of three satellites placed 22,241 miles above the equator can provide global coverage for the whole of planet Earth.
- **Radio** communications do not have to depend on microwaves or satellites for short range transmissions. Radio signals can be used to broadcast wireless transmissions through the air to connect LANs. The radio signals can usually travel through office walls and there is no need to install any wiring.
- **Infrared signals** are light signals which are not visible to the human eye but which can be used to transmit a pulsating data signal. These are most commonly used for remote controls – most television remote controls use infrared signal for example. In computing infrared transmitters and receivers can be used to connect computers and equipment at short range.
- **Cellular radio technology** is used for mobile phones. A geographical area is divided up into cells and in each cell there is a radio antenna (this might be placed on top of a tall building or mountain peak or it might be a purpose built tower). Communications from a mobile phone (or cell phone) are transmitted from antenna to antenna until they reach their destination. As well as cell phones, we now also have smart phones which can send video and can be used to connect to the Internet. People want to be able to use their PDAs and netbooks wherever they are without being physically connected to a network. Many office buildings and public buildings now offer wireless connectivity so that people can access the Internet whilst they are travelling (for example some train companies provide wireless connections for their passengers) or eating (for example in the UK many MacDonald's restaurants are now wireless *Hotspots*). We will discuss the evolution of wireless networking in section 8.5.3.

Learning activity

More and more people now have a global positioning system or GPS in their car. Write a paragraph describing how GPSs use satellites to determine their position anywhere on Earth.

8.5.3 Wireless networking generations and standards

We have already discussed the *Transmission Control Protocol* and *Internet Protocol (TCP/IP)* which enables different networks to communicate with each other. In order for wireless networks to work together another set of standards and protocols are required. Unfortunately different standards for wireless networks have been adopted in different parts of the world. There are two main standards and they usually do not allow for cross transmissions from one system to the other.

- **Global System for Mobile Communication (GSM)** – used in Europe, China, Asia and some regions of the United States.
- **Code Division Multiple Access (CDMA)** – used mostly in the United States.

There are also several generations of wireless cell technology. When cellular radio technology was first developed it was designed primarily for transmitting voice and short text messages. Nowadays people want to transmit videos, photos, connect to the Internet and generally do much more than just speak or text on their mobile phones. We are now on, or moving towards, *third generation* or *3G* wireless networks. The transmission speeds that these networks offer mean that video, graphics and other media can be sent over the network. Mobile phones, netbooks and PDAs using a 3G network are also able to connect to the Internet.

3G networks are most commonly available in South Korea, Japan and many European countries. Although 3G is not widely available in the United States, providers there have upgraded their networks to a so-called *2.5G* standard so that, although transmission speeds and capabilities are not as good as for 3G, users of a 2.5G network can still access the Internet and so on.

The next generation, *4G* is being developed and likely to be available in the next decade. 4G networks will be even faster and provide high quality and high security transmissions.

Bluetooth

Bluetooth is a wireless technology standard[2] that now comes installed on many computers and other devices. Bluetooth enabled devices can communicate with each other easily. For example just pointing a bluetooth-enabled laptop at a bluetooth-enabled printer makes them become part of a network. Bluetooth can connect up to eight devices within a 10-metre area using a low-power radio based communication signal. This makes it ideal for *personal area networks (PANS)* such as home networks where a wireless mouse, wireless keyboard, computer and printer might all be connected wirelessly using bluetooth.

Learning activity

Although it is ideal for small, personal networks, many large businesses have also found that bluetooth is a very useful tool. Describe how a restaurant could utilise bluetooth technology to make the process of getting orders from the customers to the kitchens more efficient.

[2]bluetooth is officially the 802.15 wireless networking standard

Wi-Fi

Wi-Fi(short for *wireless fidelity*) is the common name for the networking standards for wireless LANs. [3] Wi-Fi connects computers wirelessly to a wired network via *access points*. An access point is a radio receiver/transmitter that links to a wired network, router or hub. Wi-Fi can be installed on existing computers and is often pre-installed on new computers. A Wi-Fi enabled computer has a wireless NIC (network interface card) that contains a built-in radio and antenna, thus it can send and receive messages from the access point.

Access points to a Wi-Fi network are called *hotspots*. Libraries, stations and other public places may be Wi-Fi hotspots. The advantage of Wi-Fi hotspots are obvious – they are very convenient and people want to be able to access the Internet and pick up their emails etc. wherever they are. The disadvantage is that they are not that secure (it is relatively easy to *tap* into a Wi-Fi communication) and that as more people try to access the same hotspot the connection can suffer from interference. Despite the disadvantages, more and more hotspots are appearing and it is likely that sooner or later Wi-Fi will provide similar coverage to mobile phone networks.

8.6 The Internet

We have talked throughout this subject guide about *the Internet* and assumed that everyone doing a course in computing has at least a basic understanding of what we mean by the Internet.

More than one billion people now use the Internet – that is about 15% of the global population. People use the Internet for many different reasons, to email, shop, play games, study, for business, for fun, for eduction, to communicate. Hopefully you are one of them!

“Who invented the Internet?” is a difficult question to answer because no one person did. A number of people made different breakthroughs and solved different problems and as a result the Internet became possible. American textbooks are likely to say that the Internet was invented in America in 1969 but British textbooks will counter that this was only after the Internet had already been invented in England.

“What is the Internet?” is a bit easier to answer. Simply put, the Internet is a worldwide system of interconnected computers and networks. It is a huge wide area network (WAN) and is the largest implementation of a client/server network. No one has overall control of the Internet and it has no owner.[4]

[3] Wi-Fi is officially the 802.11 set of standards for wireless LANs comprising standards 802.11a, 802.11b and 802.11g. Standard 802.11n for increasing the speed and capacity of wireless networks is under development.

[4] Different parts of the Internet are owned by many different public and private bodies. In China for instance, the government owns the *backbone* of the Internet infrastructure and tries to exercise control over the Internet. In other countries the Internet infrastructure is generally privately owned.

Learning activity

By researching on the Internet or otherwise, see if you can answer the question "Who invented the Internet?".

8.6.1 Connecting to the Internet

Most small businesses and home users connect to the Internet through an Internet Service Provider (ISP) such as Virgin or Sky. Larger businesses, universities and so on may have their own designated Internet domain. Traditionally people connected to the Internet using a telephone line and a modem, but for most people this method is being replaced by broadband. Broadband connections can be provided via Digital Subscriber Lines (DSL), Cable and Satellite connections, T1 and T3 lines.

- **Digital Subscriber Lines (DSL)**– uses ordinary telephone lines to carry voice and data transmissions at high speeds.
- **Cable** – the telecommunications industry is making use of the coaxial cable that is already used by television companies to provide their customers with cable TV. This cable can also be used to provide an Internet connection. If too many people are accessing the line at the same time all will suffer progressively slower speeds, but cable is still much faster than dial-up modem.
- **Satellite** – in areas where DSL and Cable connections are not available, it is possible to connect to the Internet via a satellite link. This is slower than other other broadband connections.
- **T1 and T3 lines** – these are leased, dedicated lines which can be used by businesses or governments who require a guaranteed high-speed level of service.

8.6.2 Internet addresses

Every computer that is connected to the Internet has a unique *Internet Protocol Address* of *IP* which is a series of numbers such as 158.223.1.6. Since these IP addresses are not that easy to remember, they are converted into *domain names* such as www.londoninternational.ac.uk. Every unique domain name has a unique IP.

Domain names have a hierarchical structure and tell us a lot about the computer they are linked to. For example from the domain name *www.londonexternal.ac.uk* we can tell that this is a computer in an academic establishment in the UK. You can buy a domain name that you like the sound of, *www.topstudent.com* maybe, so long as no one else already owns it.

Learning activity

Find out the IP address and domain name of the computer that you use to access the Internet.

8.6.3 Internet services

As we have already said, the Internet is a client/server network. People using the Internet use client applications such as web browser software that is installed on their computers. Data, such as email messages and web pages are stored on servers. A client computer uses the Internet to request information from a particular web server on a distant computer. The server sends the requested information back to the client computer over the Internet. Nowadays, the client computer may not be an actual computer at all but could be a smart phone, netbook, laptop, television etc. With so many new information and communications devices now available, companies have found it necessary to upgrade their networks in order to incorporate these new technologies and keep up with their competitors.

A client computer connecting to the Internet has access to a large number of services. These include e-mail, instant messaging, newsgroups, telnet, FTP, virtual private networks and voice over Internet protocol. Will we look briefly at each of these in turn and finally consider the greatest Internet service of all – the world wide web.

Email

Email or *electronic mail* is the ability to send text messages and attachments which might be written documents, graphics such as photographs, video etc. over a network. Most email today is sent over the Internet. The advantage of email is that it costs far less to send an email message than it does to send a hard copy of the same message, and most email messages arrive within seconds of being sent irrespective of geographical distance. *Gmail*, *Yahoo* and *Hotmail* are all examples of email service providers.

Instant messaging

Some people prefer to use *chat* or instant messaging services instead of (or as well as) email. Instant messaging is especially useful for personal messages and many instant messaging services tell you when your “friends” are on-line so that you can “chat” with them. Instant messaging is more informal than e-mail – typically the messages are not saved so you cannot revisit them later. They are also more interactive – you can only “chat” with someone when you are both on-line. *MSN, Yahoo, AOL/AIM, MySpace, Facebook* and *Google Talk* are all examples of instant messaging service providers.

Newsgroups and discussion forums

Internet newsgroups provide a place where people with the same interests can log-on, read other people’s views and add their own messages to discussions. An Internet newsgroup is analogous to a bulletin board where people can stick up messages for others to read. Often anyone can read the messages that have posted in a newsgroup or discussion forum, but you may have to register with the group in order to be able to post your own messages. A newsgroup administrator keeps an eye on the message content and decides how long messages will stay visible. *Freecycle.co.uk*, which lets people advertise items that they want to give away rather than throw away, is an example of a newsgroup.

Telnet and FTP

Telnet is a client/server protocol that allows you to log-on to a remote computer system. For example, I can sit at home but use Telnet to log-on to the server at the Department of Computing at Goldsmiths. Furthermore I can use the *File Transfer Protocol (FTP)* to transfer files from one computer to the other. *FireFTP* is an example of a free FTP service that can be downloaded as an add-on to Mozilla Firefox.

Virtual private networks (VPN)

A virtual private network uses Internet technology but, as the name suggests, is private and accessible only to those who have access rights, for example those who have been issued a username and password. A company might use a VPN to communicate with its employees, suppliers and customers. Different access rights might be issued to different user types. For instance customers would not be able to access the staff information pages. The VLE (Virtual Learning Environment) for the University of London *http://computing.elearning.london.ac.uk/login/custom_login_page.php* is an example of a VPN.

Voice over Internet protocol

Using the Internet instead of the telephone has become popular over recent years. If you already have a broadband connection then there is no additional cost to send a voice message over the Internet rather than paying for expensive long distance telephone calls. Voice over Internet protocol (VoIP) technology allows voice communications to be delivered in digital rather than analogue form using packet switching. VoIP technology is basically changing the Internet into a global telephone network. The computer that you are using will need a microphone and speakers. If you also have a webcam then you can send video messages in a similar way. *Skype* and *Winkball* are examples of VoIP service providers.

8.6.4 The world wide web

In 1989, an English scientist called Tim Berners-Lee (now Sir Tim Berners-Lee) created a software program to help him keep track of information. This program eventually became the world wide web or www or *the web* for short. The web uses a client/server architecture to store, retrieve, format and display information. *Web pages* are formatted using *hypertext* and contain *hyperlinks* that connect pages to each other and to other objects such as sound, music or video files. The web is a huge repository of data and information all connected to each other by hyperlinks. It is amazing to think that just 20 years ago the web did not even exist.

We will briefly describe the role that HTTP, web browsers, web servers and search engines play in making the world wide web the incredible resource that it is.

HTTP

As mentioned above, web pages are formatted using hypertext. A *web site* is a collection of *web pages*. A web site has a short *domain name* such as www.gold.ac.uk and may be the central repository for many web pages. The URL (Uniform Resource Leader) for these pages will start with the same domain name, followed by a / and then a *path* such as www.gold.ac.uk/computing The *Hypertext Transfer Protocol (HTTP)* is the communications standard that is used to transfer webpages.

When you request a webpage by typing a URL that starts with *http://www* [5] you are requesting your web browser to transfer a webpage using http. For example if you type the URL *http://www.gold.ac.uk/computing/research/projects/* you are requesting to use http to transfer a webpage to your screen. The domain name is *www.gold.ac.uk* and the path *computing/projects* tells the browser exactly where to look on the Goldsmiths domain web server.

A URL that begins with *https* indicates that this is a site which uses secure socket layers and offers a more secure transmission protocol than http.

Web servers

All websites are stored on web server computers which store the data and have software for locating and managing the web pages. Instead of maintaining their own web server, many companies pay a web hosting service to maintain their website for them. A freeware product called *Apache HTTP Server* is the most widely used web server software.

Web browsers

A web browser is a software application that locates and presents web pages from the web. *Microsoft Internet Explorer* and *Mozilla Firefox* are two well-known examples of web browsers. Although primarily designed to work with the web, web browsers can also be used in private networks.

Search engines

There is so much information on the web that we need some way of finding what we are looking for. Search engines such as Google and Yahoo trawl through the files on the web and suggest web pages that meet your search criteria almost instantly. Most people only use one search engine but it can be worth trying different ones using the same search criteria and comparing the results.

Web search engines were originally designed to search through text documents and look for key indexed words. Nowadays, however, search engines can find specific pictures, videos and music files as well as text files and they work by indexing pages and ranking them. See *http://www.googleguide.com/google_works.html* for a description of how Google works.

[5] Most web browsers automatically add the http for you now so you can simply type the domain name.

Search engines are basically computers that do not understand human language. Many of the pages that a search engine offers you in response to a search request may be inappropriate.[6] The *Semantic web* is the name given to a collaborative effort to make the web more meaningful and reduce the amount of human effort that is currently required to sift through and process search results.

Learning activity

Do a web search to find out about the *Semantic web* and write a paragraph discussing this evolution of the world wide web.

8.7 Summary

In this chapter we have looked at the evolution of telecommunications from separate telephone and computer network systems to a merged communications system that can transmit both digital and analogue signals. We have looked at the components and topology of local area networks (LANs) and seen that a wide area network (WAN) is basically a collection of interconnected LANs. We have discussed computer network technologies including client/server computing, packet switching and TCP/IP without which the Internet – the biggest WAN of all – would not exist. We have considered different telecommunications media for both wired and wireless networks and discussed the advantages and disadvantages of these different media. We have looked at the Internet, how we can connect to it, and the services, including the web, that the Internet provides.

8.8 A reminder of your learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe how telecommunications technology has evolved over the past 20 years
- describe the component parts of a computer network and draw a simple local area network (LAN)
- describe a LAN in terms of its topology and discuss the advantages and disadvantages of different topologies
- describe the three computer network technologies client/server computing, packet switching and TCP/IP and understand how important these technologies are in enabling the development of telecommunications
- explain the difference between digital and analogue signals and why a modem is necessary to transfer between the two different types of signal
- describe the different types of communication channels that can be used for a wired network and discuss the advantages and disadvantages of each

[6] *Laudon and Laudon* suggest that you type first "Paris Hilton" and then "Hilton in Paris" into a search engine and compare the results. They suggest that you will get pages on Paris Hilton the girl in both cases because the search engine does not know that you are interested in hotels rather than the girl in the first case. Although this is true, when I tried this experiment using Google there were several pages about hotels in Paris returned for the Hilton in Paris search. It seems that Google and other search engines are becoming better at what they do.

- describe the different types of communication channels that can be used for wireless networks and discuss the advantages and disadvantages of each
- understand that the Internet is an example of a wide area network (WAN) and describe briefly how the Internet works and the services that it offers including the web.

8.9 Chapter questions

1. Describe the TCP/IP standard and discuss the advantages of a company using these standards when building a network.
2. Describe some of the Internet services that are available to businesses and explain how they can add value to the business.
3. Discuss the advantages that Voice over Internet Protocol (VoIP) technology may bring to businesses.
4. Think about a work or learning environment that you know well. How could a wireless network be used to improve communications and/or services. What current processes would have to change in order to incorporate the new wireless network and the uses that you have suggested for it? If you already have a wireless network at your place of work or study describe how has this improved communications and/or services.
5. What is the difference between the *Internet* and the *world wide web*?

Chapter 9

Information security

9.1 Introduction

In this chapter, we will discuss the security of computers and networks and the information stored and transmitted by them. We will consider the different types of attack that hackers and fraudsters can attempt and the damage that they can inflict. On a more positive note, we will discuss the steps that we can take to detect and prevent such attacks.

Essential reading

Laudon and Laudon, *Management Information Systems Managing the Digital Firm*, Chapter 8.

Additional reading

Bruce Schneier, *Secrets and Lies, Digital Security in a Networked World*, ISBN-13: 978-0471453802 John Wiley & Sons (23 Jan 2004)

9.2 Learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe why networked computers in general, and wireless networks in particular are vulnerable to security threats
- describe the damage that viruses, worms and trojan horses can do and how they are spread. Give examples of each of these
- describe the different methods that a hacker might use in order to try to gain unauthorised access to a computer network
- outline the consequences of a breach of security
- describe computer crimes including modification of data, theft of data, identity theft, cybervandalism, cyberterrorism and denial of service attacks and understand the implications for a company that is the victim of such an attack in terms of loss of finance and/or reputation
- describe how access controls such as username/password systems, firewalls and anti-virus software are used to control access to data and resources

- outline the basic principles of encryption, what it is used for and the difference between public and symmetric key encryption schemes
- describe how private encryption keys can be used to digitally sign electronic documents and produce certificates which verify public keys
- explain the importance of security policies and why companies need to make sure that their security systems provide accountability.

9.3 The importance of information security

We have talked throughout this subject guide about data and information and how important it is for companies to use information systems to gather, analyse and store data in order to gain and keep a competitive advantage. However, when data is stored electronically it is open to all sorts of threats that did not apply before the company 'went digital'. As companies become more technology oriented they need to be aware of the security and control issues that surround their information systems and provide protection from unauthorised and malicious attacks on the data that they store. There is also the need to protect data transmissions from attack, whether over wired or wireless networks to prevent unauthorised access to information.

9.3.1 Threats to information systems

Information systems are very vulnerable to attack at many levels. Any of the components of the system can be attacked as can the communication channels between them. An information system can be attacked from an external or an internal source. It is a fact that most computer crime against companies is committed by former or current employees of that company. After all, employees know the computer system best and have easy access. Therefore whilst it is imperative that companies have security measures in place to counter attacks from external sources, they also need to be aware of what their own workforce is doing and protect against attacks from within. Good access controls (see section 9.5.1) and accountability (see page 67) can help the company keep track of who is doing what, when on their computer systems. Educating the workforce in the importance of information security is also paramount because many employees may unknowingly weaken the security of the system by using easy to guess passwords or falling victim to a spoofing attack (see section 9.4.1).

Not only does the hardware and software within an organisation need to be protected. All of the mobile computing devices such as smart phones, laptops and netbooks that connect to the network are potential *points of access* to the network and as such they add to the vulnerability of the network. Wireless networks are particularly vulnerable because the idea behind them is to make access to the Internet and other networks easy but this also makes it easier for hackers to access user systems to steal data or spread malicious programs.

Specific reasons why wireless networks are vulnerable include:

- Radio frequency bands are easy to scan meaning that both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers (someone listening in on the line).

- Using an external antennae, the range of Wi-Fi networks can be extended by up to a quarter of a mile. Therefore armed with an external antennae and a laptop equipped with a wireless card and hacking software, an attacker can gain access to a local area network from some distance away.
- The aim of Wi-Fi transmissions technology is to make it easy for Wi-Fi devices to find an access point. Therefore *service set identifiers (SSIDs)* which identify the access points in a Wi-Fi network are broadcast repeatedly and so are easy for hackers to pick up whilst scanning the network. Once the hacker has identified the correct SSID for an access point they can access other devices on the network, determine which computers are connected to the network and access their hard drives.
- Hackers can also establish rogue access points called *evil twins* on different radio channels and divert signals from authentic points. They can then capture the usernames and passwords of genuine users. Public Wi-Fi hotspots are particularly vulnerable to this kind of attack.
- Although there is a security standard for Wi-Fi networks called *Wired Equivalent Privacy (WEP)*and this is built into Wi-Fi enabled products, it is not compulsory for users to use WEP. Those who do not leave their networks unprotected. Even with WEP in use, the protection that it offers is not foolproof – the 40 bit encrypted password used can be decrypted by hackers who eavesdrop on network transmissions.

As soon as you join a network to the Internet then every other computer or device on the Internet becomes a potential point of access to your network and you have to take steps to ensure that unwanted visitors are kept out. Such unwanted visitors might include hackers, various kinds of computer viruses and spyware.

Hackers

Hackers are people who intentionally gain access to computer systems without authorisation. Some hackers are simply *computer geeks* who break into systems just to show that they can. They might not be malicious in intent but they can get into a lot of trouble if they break into military or other high security systems.[1] Other hackers are malicious and they may introduce viruses, steal data or perform other criminal activities – usually for financial gain or because they hold a grudge against the organisation whose system they are hacking.

Computer viruses

A computer virus is a piece of software that attaches itself to other software programs and is executed without the user's knowledge. Computer viruses are passed from computer to computer and so spread like a cold or flu virus spreads through the human population. Some computer viruses are harmless, for example when executed they might just open a pop up window with a message in it. Others are extremely destructive and can cause all of the data on the computers hard drive to be destroyed. For example, the *ILOVEYOU* virus that was first detected in 2000 was spread as an email attachment entitled "I LOVE YOU". Opening the attachment

[1] A Scottish man, Gary McKinnon, who has Asperger's syndrome managed to hack into military computers in the USA recently. He claimed to be looking for evidence that UFOs existed. The USA military claimed that he deliberately took control of their computers and they are attempting to have McKinnon extradited to America where he could be imprisoned for a very long time.

caused the virus to overwrite the music, image and other files on your computer with copies of itself.

Worms

A worm is a malicious computer program that, unlike a virus, does not need to attach itself to another file but can operate on its own. Worms can spread more quickly than computer viruses because they do not need any human intervention to spread from one computer to another. Like a virus, worms can destroy data or halt the system by clogging it up with software generated electronic transmissions.

Trojan horses

Like the Greek Trojan Horse of history, a computer trojan horse looks like something benign or even pleasant, and turns out to be hiding something not so nice inside. For example, an electronic greetings card may conceal a virus. The *Storm* trojan horse, first detected in 2007, spread as a spam email with a fake attachment. Opening the attachment causes the computer to become affected and join a network of computers which were then used for criminal activities. At its peak up to 10 million computers were infected by Storm.

Spyware

Not all spyware is malicious or damaging, some companies use spyware to gather information on how users are navigating through their websites. On the other hand, spyware can be used by hackers as a means of installing malicious code onto a computer thereby allowing them to gain access to that computer and its associated network. **Key loggers** are a type of spyware that records every keystroke made using the computer keyboard. These can record passwords, credit card details etc making them particularly dangerous. Whether they are malicious in intent or not, spyware can cause computers to become very slow as they overload the memory.

Learning activity

Find an example of a computer virus (other than I LOVE YOU) and describe how it is spread, what damage it does, how many computers are estimated to be (or have been) infected by this virus. What do you think was the aim of the designers of your chosen virus?

9.4 Consequences of poor security

If poor computer security allows a hacker or a virus to gain access to your network, then the consequences might include:

- unauthorised access to, modification and theft of information
- disruption of communication

- identity theft
- cybervandalism
- denial of service.

Any of the above will have implications for the finances and reputation of the company. It is therefore very important that the company does its utmost to prevent such attacks. Below we discuss the various consequences of poor security in more detail. In section 9.5 we will describe the measures that companies and individuals can take in order to keep their information and networks secure.

9.4.1 Unauthorised access to information

A hacker might gain unauthorised access to an information system perhaps by using spyware as described above to find out the log-in details of an authorised user. The hacker might set up a **spoof** website which looks almost exactly like the genuine log-in screen for the network. The user, unaware that their computer has been tampered with, enters their username and password. They are then given a message to say that their log-in attempt was invalid and they should re-enter their details. The user cannot be sure that they did not make a mistake when entering their details so they re-enter them and gain access to the network. What the user does not realise is that the first time they tried to log-in, they were actually entering their details onto a spoof site. These details have been captured by the hacker and then the real site is loaded so that the user can log in as usual and will not suspect that anything untoward has occurred. Spoof sites are also used to gather financial information such as bank account details.

Another form of spoofing is called **phishing**. Fake emails, which look like legitimate business emails, are sent to people asking for personal details such as name, address, bank details etc. The user may think that the email is genuine and respond thereby sending their personal information directly to an attacker. This attack will be particularly effective if the attacker already knows some information about their target. For example, suppose you place an order over the Internet with an e-commerce company. A hacker has listened in to transmissions and guesses that you have placed an order with the company but because the transmission was encrypted they cannot get your bank account details from the information that they have eavesdropped. However, they do know your email address and the time and date of your order. The attacker might email you, pretending that the email comes from the company. They tell you that the order that you placed at a specific time on a specific date has not gone through because of a problem with their computer system and that they therefore need you to resend your payment details by replying to the email. You may be fooled into emailing your bank details straight to the attacker!

Hackers might also use **Sniffer programs** which pick up information as it is passed over transmission channels, both wired and wireless. It is very hard to detect sniffer programs. However the hackers can be thwarted if encryption (see section 9.5.2) is used to make any information that the hackers get unreadable and therefore useless to them.

Note that the easiest way for a hacker to get hold of someone's password is usually to ask them. Most people are badly educated about computer security and will willingly tell other people their password. For example, imagine the following scenario. A hacker phones someone at their work desk and says that he is from the computer systems department. He tells them that there is a problem with the system and that

he needs to know their password in order to save all of their files before the system goes down. Many people fall for this kind of trick and reveal their passwords.[2] Educating the work force is probably the most important part of information security.

If the hacker is from inside rather than outside the company then they may simply *shoulder surf* to try and find out their colleagues log-in details by watching them type them in. If an employee logs in to their own work system using someone else's log-in details this means that not only will they gain access to their colleague's files but they will also be able to make changes to the system without being held accountable – all audit trails and checks will point to the person whose log-in details have been used.

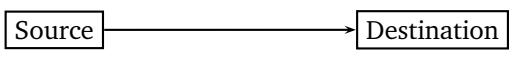
Once they have gained unauthorised access to an information system, what might the hacker do?

- Read information – such as bank details which they can later use to steal money from people's bank accounts or purchase items using stolen credit card details.
- Modify information – for example changing the payee details on an order to transfer money from one account to another so that the money is diverted into their own account.
- Delete information – this might not directly cause a financial gain to the hacker but they might have a grudge against the company and wish to cause them trouble.
- Steal information – in the case of computer crime stealing information is basically the same as reading it. It can be hard to detect theft of information because unlike stealing a physical item you can steal information whilst still leaving it in place simply by reading or copying it. If a physical item such as a car is stolen there is no problem in noticing the crime – your car is missing. If computer files are stolen by copying then there may be no evidence to indicate that a theft has taken place. Furthermore, if a thief steals your car you at least know where he was at the time of the theft – wherever your car was. If a thief steals your computer files he may be on the other side of the world whilst doing it. This makes it hard to know who is responsible for catching a computer criminal. Is it the police in the country where the computer is, or the police in the country where the criminal is? We will discuss international security policies that try to address this question in section 9.6.

9.4.2 Disruption of communication

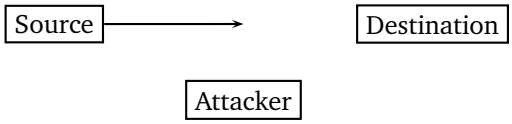
An attacker can disrupt communications over a network in a number of ways. Information can be *interrupted*, *intercepted*, *modified*, or *fabricated* as illustrated below.

If everything is going as planned, information is transmitted from the source to the destination.

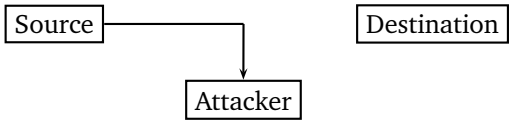


[2] In 2004 an experiment was carried out at a London railway station. A small group of researchers asked commuters to reveal one of the passwords that they used at work in exchange for a bar of chocolate. Over 70 percent of the commuters gave a password away. Some of these may have been false because there were no checks done to verify that the passwords were genuine. However it is likely that a great many real passwords were revealed.

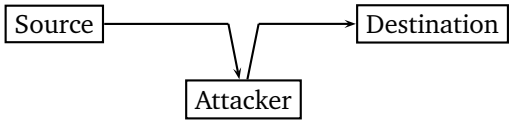
Communication is *interrupted* if the attacker does not allow the information to reach the destination.



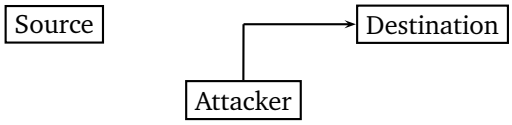
Communication is *intercepted* if the attacker interrupts the communication and receives the source information.



Modification occurs when the attacker intercepts the communication, alters it in some way, and then sends it on to the destination. The attacker intends to deceive the destination into thinking that the modified communication has come directly from the source. This is also known as a *Man-in-the-middle attack*



An attacker may also make up a communication and send it to the destination pretending that it has come from the source. This is called *fabrication*.



Learning activity

For each of the ways that an attacker might disrupt communications described above (interruption, interception, modification, fabrication) think of an example of a reason why an attacker might want to interrupt communications in this way. What does the attacker gain?

9.4.3 Identity theft

One of the fastest growing crimes is *identity theft* whereby someone gathers enough information about you to pretend to be you. The information might include your name and address, credit card details, social security or national insurance number, drivers licence or any other information that they can use to "prove" that they are you. Armed with this information, an identity thief can obtain credit, buy goods and services, perhaps even travel or get a job illegally because they are acting as you.

Identity theft can occur off-line – simply going through a dustbin is likely to yield lots of information about the people who live in that house. Hence the thief has the address (he knows where the dustbin is) and probably the names and perhaps other details about the occupants. Discarded bills, bank statements and letters all reveal a great deal that is useful to an identity thief. Identity theft can also occur on-line by hackers using phishing and spoof websites or rogue Wi-Fi access points to get personal information about people.

Although the original theft might occur off-line, once your personal information has been stolen, it is easy for the thief to use it on-line.

There are many precautions that people can take to prevent themselves falling victim to identity theft:

- Shred all documents containing any personal information before putting them in the dustbin.
- Be very wary about any emails or phone calls that ask you for personal information, especially financial information. No financial institution will ask you for your account information by e-mail. If in doubt say that you will phone/email back using a number/e-mail address that you already have – not one given to you by the caller.
- Never give out any personal information unless you have initiated the transaction.
- Keep your computer security software up to date to prevent hackers accessing your information.
- Keep a check on your credit rating – if you suddenly have a lot of debt that you are not aware of you may have been the victim of an identity thief and should report this immediately.

9.4.4 Cybervandalism

Just as vandals destroy physical items with no particular purpose, cybervandals can destroy websites just because they think it is fun or because they hold a grudge against the company. If a hacker manages to alter a company website and fill it with offensive material and language this can have dire consequences for the company. Tight access controls need to be enforced to ensure that no one can alter a company website, the public face of an e-commerce company, without the proper authority.

9.4.5 Denial of service attacks

Denial of service attacks do not destroy or access information without authority. What they do is prevent anyone else from accessing that information. A denial of service attack might be carried out by the attacker flooding the system with requests until it can not keep up with the demand and crashes. Legitimate users are then unable to access the system. Consider the damage that such an attack might have on an e-commerce site such as an Internet shop.

The attacker might initiate a denial of service attack by using a virus or worm which causes infected computers to join a *zombie network* or *botnet* which continually requests access to the target network.

Learning activity

On 6th August 2009, the social networking site, *Twitter* was shut down for several hours due to a denial of service attack. Learn more about this attack at http://community.norton.com/t5/Ask-Marian/Twitter-Hit-By-Distributed-Denial-of-Service-Attack-DDOS-Attack/ba-p/128035. What was the aim of this attack? What are the implications for *Twitter*?

9.4.6 Cyberterrorism

Nearly all of the threats mentioned so far – denial of service attacks, viruses, worms, unauthorised access to information, communication disruption and cybervandalism – can occur from anywhere in the world. As terrorism continues to increase, governments are worried that computer systems are as likely to be attacked as buildings, cars or trains. The benefit for the terrorists is that they do not have to be anywhere near the computer system that they are attacking. Widespread disruption and harm could be caused if cyberterrorists were able to manipulate military, air traffic control, financial, or foreign intelligence systems for example.

Read more about Cyberterrorism and how we can defend against it at www.symantec.com/avcenter/reference/cyberterrorism.pdf.

9.5 Keeping information secure

We have discussed some of the threats that companies are up against when trying to protect their information and networks against attack. In this section we will look at ways in which companies can minimise attacks by using *access controls* to prevent unauthorised access to the network and *encryption* to prevent any data that is leaked during transmission or stolen from a network from revealing anything of use to the attacker.

As mentioned before, employees are the people who are most likely to cause security breaches in a company. This might be with intent or by accident. Educating your staff in computer security and enforcing security policies, for example on password choice, is as important as having the policies in the first place.

It is a big job to effectively manage all of the different security tools that are available to businesses. *Unified threat management* technologies such as those provided by *Crossbeam*, *Fortinent* and *Secure Computing* help businesses by providing all of the necessary security tools in one comprehensive package. This can be an efficient way for a small to medium sized business make sure that they have covered all of the security vulnerabilities in their computer systems.

9.5.1 Access control

Security of data and networks depends upon the proper implementation of access controls. Broadly speaking, access control means that people who have the proper

authority should be able to do whatever it is (and only whatever it is) they are authorised to do. Nobody else should be able to do anything on the system.

Within a company, different users may have different access rights to the information system. Consider the University of London Computing VLE for example (http://computing.elearning.london.ac.uk). Access to the VLE is controlled by username and password. Only students, academic staff and administrative staff are issued with a username and password and so only they can access the VLE. Different users have different access rights. For example, students can access only the courses that they are registered on. They can upload their own assignments and write or reply to questions in the forums for their courses and the general student forums. However students are not able to edit the website or add new courses. Some staff are able to access the site but have read only permission – they are not able to join in the discussion forums but can use the site for information only. Administrators are able to access all of the courses, edit the website, add users and courses and so on.

Username/password systems

The most common method for implementing access control is a username/password system as used in the VLE. The *username* provides *identification* – it tells the system who you are and associates you with the correct access permissions. The *password* provides *authentication* – it proves to the system that you are who you say you are.

Getting hold of somebody's username and password is the easiest way for a hacker to gain access onto the system. Many users choose *weak* passwords that are easy for a hacker to guess. Such weak passwords include:

- No password at all – some systems allow the password field to be blank – a blank password offers no security at all.
- A short password – in general the longer the password the harder it is for a hacker to *break* the password using a password cracking program that tries all combinations of characters. Consider that if a password is 4 characters long and is made up of upper and lower case letters (52 different characters in all) then there are $52^4 = 7,311,616$ possible passwords. It would take a password cracker less than a second to check all of these. On the other hand, if the password is 8 characters long then there are $52^8 = 53,459,728,531,456$ possible passwords and it will take considerably longer to check all of these.
- A dictionary word – before resorting to trying all combinations of characters a hacker will usually perform a dictionary search. He will simply use a computer program that tries all dictionary words as the password. The number of eight letter words in a English dictionary is a lot less than 52^8 and it will not take the hacker long to try all of them as the password.
- A personal password – many people use a password that is related to them in some way, perhaps the name of their pet or their favourite football team. Such passwords are easy to remember but they are also easy for a hacker to guess – especially if the hacker is a work colleague!

Password systems are only as good as the passwords used. To counter this, security experts are coming up with alternative methods for authentication. Such methods include using *tokens* and *smart cards* which are small physical devices that act a bit like a key and allow the holder access to the network. Work is currently being done on the use of mobile phones as tokens.

Biometric information such as fingerprints, retina patterns and palm prints can also be used to authenticate users. This is a high-cost solution and so would only be used when the need for security is extremely high. It is worth noting however that with sufficient financial resources a determined attacker can replicate these physical attributes, potentially leading to the catastrophic failure of a supposedly high security identity system.

Firewalls

A firewall is a combination of software and hardware that is installed in a network to control the packets of data passing through it. Most companies place a firewall at the Internet access point of their network. The firewall provides a defence between the company network and the Internet or any other network that the company's network is communicating with. All data from or to the network must pass through the firewall and only data that meets the company security policy will be allowed through. Thus the firewall prevents unauthorised communications into and out of the network.

Different firewall technologies include:

- *Packet filtering* – header fields of the transmitted data packets are examined.
- *Stateful inspection* – packets are accepted or rejected depending on whether or not they are part of a verified exchange of information between sender and receiver.
- *Network Address Translation (NAT)* – the IP addresses of the company computers are concealed to prevent sniffer programs from finding out the IP addresses and using them to help break into the network.
- *Application proxy filter* – a substitute message is passed through the firewall instead of the actual message.

Usually these different technologies are used together to provide a strong firewall. The security administrator must maintain a detailed lists of people, applications and addresses that are to be allowed or rejected by the firewall. Simply having a good firewall is not enough to guarantee that an attacker cannot gain access to the network. A firewall is an important part, but not the only part, of a good security system.

Anti-virus software

Any computer that is connected to the Internet (and even those that are not if any files from another computer are ever transferred via disks or memory sticks) should have anti-virus protection installed. Anti-virus software checks computer drives and every incoming file for known computer viruses. If you try to download or open an infected file, the anti-virus software should warn you and give you the option to delete the file or try and clean it removing the virus. Anti-virus software can only check for viruses that it knows about. Since new viruses are being released all the time, it is very important that anti-virus software is kept up to the minute by online updates. Many anti-virus software products automatically check for updates every time the computer is on and connected to the Internet.

Some anti-virus software now searches for spyware as well as viruses. As mentioned previously, not all spyware is malicious but some is. Even non-malicious spyware can

cause computers to slow down because it uses up too much memory. It is a good idea to scan your computer for spyware and remove all spyware on a regular basis if your anti-virus software enables this.

Examples of well known anti-virus software are produced by *McAfee* and *Symantec*.

Learning activity

Do you have anti-virus software installed on your computer? If no then get some now! If yes, what does your anti-virus software claim to do? Is it effective? Have you ever had a computer virus? If so how did you get rid of it?

If possible, scan your computer for spyware. Is there any spyware lurking on your computer? If so do you know where it came from? Remove it if possible.

9.5.2 Encryption

Encryption is the process of transforming a *plaintext* message (a message that can be read) into an unreadable encrypted form called a *ciphertext* message. The intention of encryption is to ensure that if the encrypted message is intercepted then it will not reveal anything meaningful to the interceptor.

Transmissions over a wireless network are particularly vulnerable to interception. As more and more wireless access points spring up over the country the vulnerability of wireless communications grows. Messages that are encrypted can still be intercepted but will reveal no important information to the interceptor.

The standard methods for making on-line transmissions more secure are **Secure Sockets Layers (SSL)** and **Secure Hypertext Transfer Protocol (SHTTP)**. If you are on an e-commerce website and the address shown in your web browser begins with https then the website is using one of these two security measures. SSL (now being succeeded by **Transport Layer Security (TLS)**) enables client and server computers to manage encryption and decryption protocols as they communicate with each other during a secure web session. SHTTP also encrypts data transmissions over the Internet but it works on a message-by-message basis whereas SSL establishes a secure connection between two computers. The ability to establish secure transmissions is built in to browser software. The user does not have to know or remember any keys or know how to encrypt or decrypt messages.

As well as protecting messages in transmission, encryption should be used when storing confidential or sensitive data. For example, in a username/password system, the passwords have to be stored somewhere in order to check them against the password that the user inputs. If the passwords are stored unencrypted in a *password file* then anyone who gains access to that file has access to all of the system passwords. Instead, the passwords should be stored in encrypted form indexed by username. When a user logs onto the system, they enter their username and password. The entered password is encrypted and the result is compared with the encrypted password stored with the given username. If these match then the user is authenticated. If not the log-in attempt is rejected. If anyone gains access to the password file, they will only see the encrypted passwords and these cannot be used to gain access to the system without first being decrypted – a very hard task is a *one*

way function (see the next learning activity) is used for the encryption.

Medical, military, financial and other sensitive records and data should also be encrypted before being stored in digital form.

There are two types of encryption schemes in use – *public key* and *symmetric key*. We will briefly discuss how each of these work and what they are used for.

Public key encryption

In public key encryption schemes there are two keys – a public key which anyone can know, and a private key which the key holder must keep secret. The two keys are related by a special mathematical function called a *one-way function* which is easy to compute in one direction but very hard (impossible in a realistic time frame) to reverse.

Learning activity

An example of a mathematical one-way function is multiplication/factorisation. Given two very large prime numbers[3], it is easy (using a computer) to multiply them together. However, it is very hard (even using a computer) to factorise (i.e. find the divisors) of the result.

For example, use a calculator to multiply together the prime numbers 1009 and 1019. This should not prove to be too difficult.

Now try to find the two prime numbers that when multiplied together give the result 5921449. This is a much harder problem. If you write a computer program which tries to divide 5921449 by all possible factors starting at 2 and increasing until you find a factor, you will be able to solve this problem. However note that the prime numbers used in commercial encryption schemes are approximately 200 digits long and this makes the factorisation problem as good as impossible to solve.

Messages which are encrypted with a public key can only be decrypted by using the corresponding public key. So if Alice wants to send Bob[4] a message, she will look up Bob's public key, use it to encrypt the message and send the resulting ciphertext to Bob. Bob receives the ciphertext from Alice and uses his private key to decrypt the message. This is illustrated in figure 9.1. Only Bob is able to decrypt the encrypted message, so even if the ciphertext is intercepted during transmission it will not reveal any information to anyone except Bob.

Public key cryptography is relatively slow and expensive when compared with symmetric key cryptography (see below). It is generally used for encrypting short messages such as keys for use in a symmetric key cryptosystem. It is also used to produce digital signatures and certificates.

[3] A prime number is a number with exactly two factors 1 and itself. The first 10 prime numbers are 2,3,5,7,11,13,17,19,23 and 29.

[4] Alice and Bob are used in cryptography to represent any two entities who want to send and receive encrypted messages. Alice and Bob could be people, companies or computers.

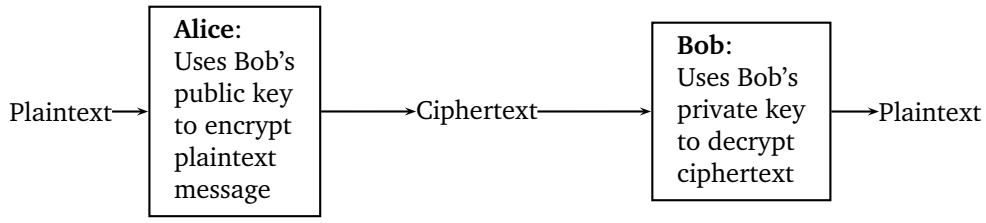


Figure 9.1: The public key is used to encrypt and the corresponding private key is used to decrypt in a public key cryptosystem

Digital signatures

If you sign your name on a document, your signature is binding and proves that you have agreed to whatever it is that you are signing. For example, if you sign a cheque then you are agreeing to pay a certain amount of money to a specified person or company. However, if you send money or important information digitally over the Internet then it is not possible to provide a hand written signature. Digital signatures are used instead.

If Bob wants to sign an electronic message for Alice, he can encrypt it using his **private key** to produce a cipher text which is the digital signature. Bob sends the cipher text and the original unencrypted message to Alice. Alice uses Bob's **public key** to decrypt the digital signature and checks that it matches the original message. If it does then Alice is assured that the message is genuinely from Bob because only he had the private key that could produce the cipher text that decrypted correctly using Bob's public key. This is illustrated in figure 9.2.

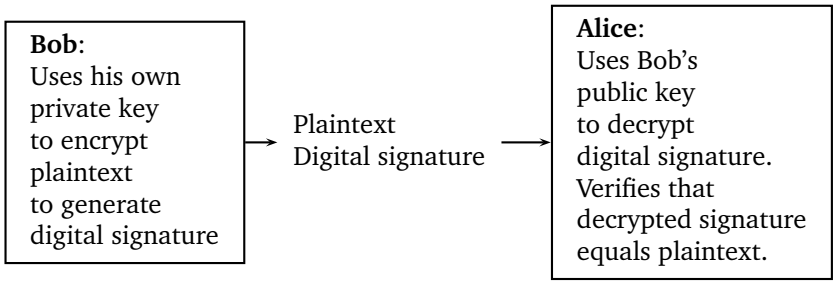


Figure 9.2: The private key is used to encrypt a message to generate a digital signature. The corresponding public key is used to decrypt the signature and verify the message.

In the scheme described above the message is sent in an unencrypted form with the signature. The message is not secret or confidential – it is just important that Alice is sure that the message has come from Bob and not from an impostor pretending to be Bob. If the message is confidential then Bob can use Alice's public key to encrypt the plaintext message and the signature. Alice decrypts the whole ciphertext using her own private key to get the message and the signature. Then she decrypts the signature using Bob's public key. If the decrypted signature matches the message

Alice is sure that the message has come from Bob and no one else who intercepts the message will be able to read it.

Digital certificates

One problem of using public key cryptography is that when encrypting a message for Bob, Alice must be sure that it is actually Bob's public key that she is using. A hacker could try to fool Alice into using his own public key in place of Bob's. Then the hacker will be able to decrypt the messages using his corresponding private key. Digital certificates are a way of ensuring that public keys are genuine.

To obtain a digital certificate, Bob produces a document which includes his name and his public key. This document is digitally signed as described above by a *certification agency* (a government agency or financial institution for example) who first check that Bob's documents and details are genuine. The signed document is the digital certificate. If Alice wants to send a message to Bob she can look up his digital certificate, decrypt it using the public key of the certification agency and use the public key for Bob contained within. In this way Alice is assured that she is using the correct key for Bob because it has been verified as genuine by the certification agency.

Public key infrastructure (PKI) which uses public key cryptography and digital certificates is now commonly used in e-commerce.

Symmetric key encryption

In symmetric key cryptography the encryption and decryption keys are the same (or one can be easily derived from the other). Hence the key must always be kept secret. If Alice and Bob want to send encrypted messages to each other using symmetric key encryption then they both need to have a copy of the key. Public key cryptography can be used to transmit the key from Alice to Bob or vice versa. Once they are both in possession of the key, Alice and Bob can then proceed to use symmetric key cryptography to transmit messages.

The advantage of symmetric key cryptography over public key cryptography is that is it faster and cheaper to use. Symmetric key cryptography is therefore generally used to transmit long messages.

9.6 Security policies

As discussed in the previous sections of this chapter there are both many threats to the security of computer networks and also many precautions that can be taken to minimise the risk of these threats. For a company to ensure that it is doing everything that it can to minimise threats it needs to have a security policy which describes the security methods and procedures that it will enforce.

It can be hard for governments to legislate effectively against computer crime because of the global nature of the problem. Criminals committing computer crime do not have to be anywhere near the scene of their crime. So is it the country where the criminals are, or the country where the crime is carried out, that is responsible

for bringing the criminals to justice? These two countries might easily have different laws and attitudes to punishment.

In the following sections we will consider the steps that companies and governments can take in the attempt to stop computer crime.

9.6.1 Company security policies

If they were building a new office block, a company would incorporate security measures into the design. From the start of the building work until the building was occupied and beyond the company would want to ensure the security of the building. It would use locking doors and windows to prevent unauthorised access, maybe install security cameras to monitor who is where in the building and make sure that no uninvited visitors have gained access. It may also have security guards patrolling the building or checking the credentials of visitors and staff so that no-one is allowed to enter the building unless they are authorised to do so.

When designing an information system a company needs to take similar steps to ensure security. Right from the start of the design process the company needs to think about how it will secure its networks and the data that it stores. Two types of information system controls are:

- **General controls** – manual and automated controls which govern the design, security and use of computer programs and data files throughout the company. General controls will apply to all computing devices and applications within the company including software, hardware, computer operations, data security, implementation processes and administrative processes.
- **Application controls** – application specific controls which ensure that input, output and processing is carried out accurately by that application.

Risk assessment

Before and during the development of information systems, businesses need to carry out risk assessment procedures to determine weaknesses in the system and the level of risk if a particular activity or process failed for security, technology or other reasons. Table 8.4 on page 340 of Laudon and Laudon shows the estimated loss of income that could occur in an online order processing system that processes 30,000 order per day. A risk assessment of this system shows for example that there is a 30% chance of a power failure and that the resulting loss of annual income might be $30,750.

Once risks have been identified, the information system designers should concentrate their efforts on those areas with the greatest vulnerability and the greatest potential for loss. For example, if a power failure would be catastrophic (suppose that the information system in question is a life support machine or the braking system for a high speed train for example) then provisions should be made for an emergency power supply in the case that the main power supply fails. **Disaster recovery planning** and **business continuity planning** give the company the opportunity to think in advance about how they would recover and continue to operate their business in the event of a disaster such as a fire or flood which leads to loss of equipment, buildings or personnel.

Learning activity

Consider the following types of businesses:

- Internet banking – enabling financial transactions to be processed on-line.
- E-commerce shop – selling goods via an on-line shop.
- An on-line magazine – provides access to subscribers via a username/password system.
- A political party or a charity that uses a website to advertise it's policies and aims.

Which of the following threats do you think would be most serious for each of these types of businesses and why? Consider this question both in terms of the cost of potential financial losses and the cost of loss of reputation.

- Unauthorised access to data.
- Disruption of communication.
- Cybervandalism.
- A denial of service attack.
- A virus that deletes all files on infected computers in the system.

Once the risks to an information system and their potential consequences for the company have been identified, the company needs to develop a **security policy** which states their security goals and how these are to be achieved. The security policy might include:

- An **Acceptable use policy** which outlines acceptable and unacceptable uses of hardware and telecommunications equipment. It might specify specific consequences for non-compliance.
- An **Access control policy** or **Authorisation policy** which determines the access different users have to different information resources.

Accountability

There is no point in having a security policy detailing who can do what, when and where if you have no way of actually knowing who is doing what, when and where. *Accountability* means that the system is able to provide audit trails of all transactions. Information system managers are accountable through scrutiny from outside of the system and must be able to provide details of all transactions that have occurred. Audit trails must be kept (and protected to ensure that they themselves are not tampered with) so that actions affecting the security of the system can be traced back to the responsible party.

Computer forensics is the collection of evidence from computers or computing devices that can be used as evidence in a court of law. It is a growing field because of the increasing use of digital storage and reliance on e-mail as a means of communication. Courts are now likely to accept all forms of communication to be used as evidence. It is therefore up to businesses to develop methods of capturing and storing all electronic communications including e-mail, instant messaging and e-commerce transactions. Anyone tempted to commit computer crime should be aware that computer forensics enables the recovery of computer files that have been

deleted because ambient data remains in magnetic form on the hard drive long after the file has been deleted.

9.6.2 Government security policies

Some companies may be unwilling to spend a great deal on implementing security polices for their information systems because such spending does not directly produce an increased revenue. Protecting information systems is vital however as the consequences of not doing so can be very damaging as discussed above – it might also prove to be illegal. So much personal and financial information is now maintained electronically that many governments have passed laws mandating how such data will be protected from unauthorised or illegal misuse.

Learning activity

On pages 336 and 337 of Laudon and Laudon recent U.S. government regulations are described:

- **HIPAA** which protects medical and health care data.
- **Gramm-Leach-Bliley Act** which requires financial institutions to ensure the security and confidentiality of their customer data.
- **Sarbanes-Oxley Act** which requires companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally.

Are there similar acts or laws in your country? Find out about them.

9.7 Summary

In this chapter we have discussed the different threats that put computers and the data stored upon them at risk. We have seen how networks may be attacked and looked at the reasons why wireless networks are particularly vulnerable. We have described how hackers and computer criminals might attempt to gain unauthorised access to data using spoofing, phishing and sniffer programs and discussed the consequences of such a breach of security. We have talked about viruses, worms, trojan horses and spyware and how damaging these can be. We have also discussed other computer crimes including identity theft, cybervandalism and denial of service attacks. We have described how companies and individuals can respond to these threats by using access controls, username/password systems, firewalls, anti-virus software and encryption. We have seen why companies should implement a security policy which sets out how the company protects its data and computers both for their own good and to meet legal requirements.

9.8 A reminder of your learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe why networked computers in general, and wireless networks in particular are vulnerable to security threats

- describe the damage that viruses, worms and trojan horses can do and how they are spread. Give examples of each of these
- describe the different methods that a hacker might use in order to try to gain unauthorised access to a computer network
- outline the consequences of a breach of security
- describe computer crimes including modification of data, theft of data, identity theft, cybervandalism, cyberterrorism and denial of service attacks and understand the implications for a company that is the victim of such an attack in terms of loss of finance and/or reputation
- describe how access controls such as username/password systems, firewalls and anti-virus software are used to control access to data and resources
- outline the basic principles of encryption, what it is used for and the difference between public and symmetric key encryption schemes
- describe how private encryption keys can be used to digitally sign electronic documents and produce certificates which verify public keys
- explain the importance of security policies and why companies need to make sure that their security systems provide accountability.

9.9 Chapter questions

- Why are wireless networks more susceptible to security threats than wired networks? What can businesses do to prevent or detect an attack on their wireless networks?
- What is a denial of service attack? Find an example of a denial of service attack and describe the impact that the attack had on the company in question. What can companies do to prevent denial of service attacks?
- Discuss the statement: Employees are the biggest threat to information security.
- What are the main differences between the theft of a physical item such as a car and the theft of an electronic item such as a secret recipe?
- Every business should have a security policy. What elements should a good security policy include?

Chapter 10

Developing information systems

10.1 Introduction

In this chapter, we will discuss the different methods that can be used to help companies develop new and existing information systems. We will look at the traditional approach which involves moving through a sequence of well defined stages, starting with system analysis and design and ending with system conversion, production and maintenance. We will compare this traditional approach with alternative methods that may be quicker and less expensive, but are also less structured and harder to control. We will see that handing control over to the end users, rather than technical specialists, results in the development of systems which meet their user requirements well, but can lead to incompatibility and poor documentation.

Essential reading

Laudon and Laudon, *Management Information Systems Managing the Digital Firm*, Chapter 13.

Additional reading

Turban and Volonino Technical Guide 5 from the student companion website for *Information Technology for Management*. This can be found at http://bcs.wiley.com/he-bcs/Books?action=resource&bcsId=4953&itemId=0470400323&resourceId=17218&chapterId=48688.

10.2 Learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe the types of organisational change: automation, rationalisation of procedures, business process re-engineering and paradigm shifts, that may come about through the introduction of new information systems
- give examples of companies that have successfully gone through the process of business process re-engineering or paradigm shift
- explain why business process re-engineering fails in many cases and describe some of the reasons for the high failure rate
- explain the importance of quality management and the steps that companies can take to enhance the quality of their services and products

- describe the six stages (systems analysis, systems design, programming, testing, conversion, production and maintenance) of a traditional systems development life cycle
- describe alternative methods for developing an information system and discuss the advantages and disadvantages of each.

10.3 New systems and organisational change

Information technology changes organisations – hopefully, but not always, for the better. Introducing a new information system will have an effect on the hardware, software and people in the organisation. It is something that has to be done in order for companies to stay or get ahead of their competitors. However, if done badly, the changes caused by the new information system can actually have the opposite effect to that desired and cause the company to fail. Managing hardware and software changes is probably easier than managing changes to the way in which people use that hardware and software. If, for whatever reason, the workforce is unwilling or unable to use the new technology effectively then it is potentially a disastrous waste of money and resources. Understanding and incorporating changes in the social and political climate of any organisation is key to success.

Figure 13.1 on page 509 of Laudon and Laudon shows four types of organisational change and the potential amount of risk and reward associated with each.

- **Automation** – using technology to perform tasks previously carried out by people. Automation is generally the easiest application of technology and the most common form of change. People usually accept that automation is a good thing – unless of course they are being made unemployed because a machine can now do their job.
- **Rationalisation of procedures** – examining standard operating procedures and removing those that are no longer necessary. Rationalisation aims to make the company more efficient. Automation can cause bottlenecks in productions since some jobs are now performed more quickly than before. The old operating procedures may no longer be the most efficient. Rationalisation is a way to streamline operating procedures.
- **Business process re-engineering (BPR)** – a total evaluation of the way in which the company works. BPR can cause major upheaval. The idea is to analyse, simplify and redesign business processes and then cut costs by eliminating unnecessary staff and processes. Employees may see this as *downsizing* the company and fear for their jobs. Very few companies are run as efficiently as possible. BPR aims to find improvements or even new opportunities for the company. The introduction of paperless billing is an example of BPR which makes use of new technology to improve efficiency and reduce costs (it is better for the environment too). *Work flow management software* can be used to help streamline procedures for companies whose primary business is based around paperwork. Laudon and Laudon give the example of how the application process for a mortgage has been streamlined and made much faster and more user friendly as a result of using work flow and document management software.
- **Paradigm shift** – changing the very nature and structure of the company by introducing totally new products or services. This type of organisational change causes major disruption to the company.

If business process re-engineering and paradigm shifts are so disruptive, why do companies undertake them? The answer is that they have to in order to cut their costs and remain competitive. The Internet is causing many different types of businesses to alter both their products and services and the way in which these are delivered.

Learning activity

Consider the music industry as an example of paradigm shift and business process re-engineering that we have been discussing. Traditional music outlets such as high street shops have been hit heavily by competition from Internet shops and music download sites. This in turn affects the way in which music is distributed. Think of one type of company affected by the change in the way that music is now bought, perhaps a shop, distributor or even a musician, and describe the type of paradigm shift or business process re-engineering that the company has made in order to survive this change.

10.3.1 Business process re-engineering and business process management

Attempts at business process re-engineering fail over half the time. Reasons for this high failure rate include:

- lack of planning
- inability to fully comprehend the size and complexity of the task
- underestimation of the time required.

To make business process re-engineering a success, the company should first decide which business processes it needs to focus on and then decide how improvements to these processes will help the company's overall business strategy. It may be helpful to draw a diagram of how the companies processes work now and how they will work after they have been redesigned. Figure 13.2 on page 512 of Laudon and Laudon gives an example of how a mortgage processing system has been redesigned using business process re-engineering techniques.

Even seemingly simple processes can involve a great many steps. **Business process management (BPM)** involves analysing every task in a business and helping companies to optimise them. BPM includes work flow management, business process modelling, quality management, change management and standardisation of processes throughout the company. To stay ahead, every company should constantly analyse how each task is accomplished and look for ways of improving.

10.3.2 Quality management

Another area of continual process improvement is quality management. As well as improving their business processes to optimise efficiency and cut costs, companies also need to improve and maintain the quality of the services and products that they offer. **Total quality management**, making everyone in the company responsible for quality control, relies on excellent information systems that keep workers and managers informed with the data necessary to improve products and performance.

Ways in which companies can use information systems to help achieve total quality management include:

- simplifying processes by using information to determine what steps are included in each process
- identifying benchmark targets
- gathering, processing and storing customer feedback in systems that are available throughout the company
- providing information earlier in the business process
- redesigning the product or process by using information about the process
- improving production processes by using information from both internal and external sources.

10.4 The systems development process

Systems development includes every resource and every step that goes into producing an information system that solves a problem or helps a company to take advantage of a new opportunity. *Laudon and Laudon* identify six core activities that make up the system development process. These are:

- systems analysis
- systems design
- programming
- testing
- conversion
- production and maintenance.

In figure 13.3 on page 516 of Laudon and Laudon these are presented as a circle. You can also think of them as a waterfall with one step flowing into the next. Be aware however that from any step you may have to go back to previous steps before you can carry on to the next step. This is shown in figure 10.1.

We will look at each of the six core activities in the following sections.

10.4.1 System analysis

A proper understanding of the business problem to be solved, or the opportunity to be grasped, is key in developing a successful information system. The system analysis should start by defining the business problem (or opportunity). Once the problem has been fully understood and considered from different perspectives (from the point of view of the company, its competitors, and its customers, for example) then potential solutions can be proposed.

Next an assessment of these proposed solutions is required. A *feasibility study* should be carried out to help determine if the proposed solution is achievable. The feasibility study will review the technical, financial and organisational feasibility of the proposal in terms of hardware, software and people and determine its probability of success. Done properly, the feasibility study can prevent the company

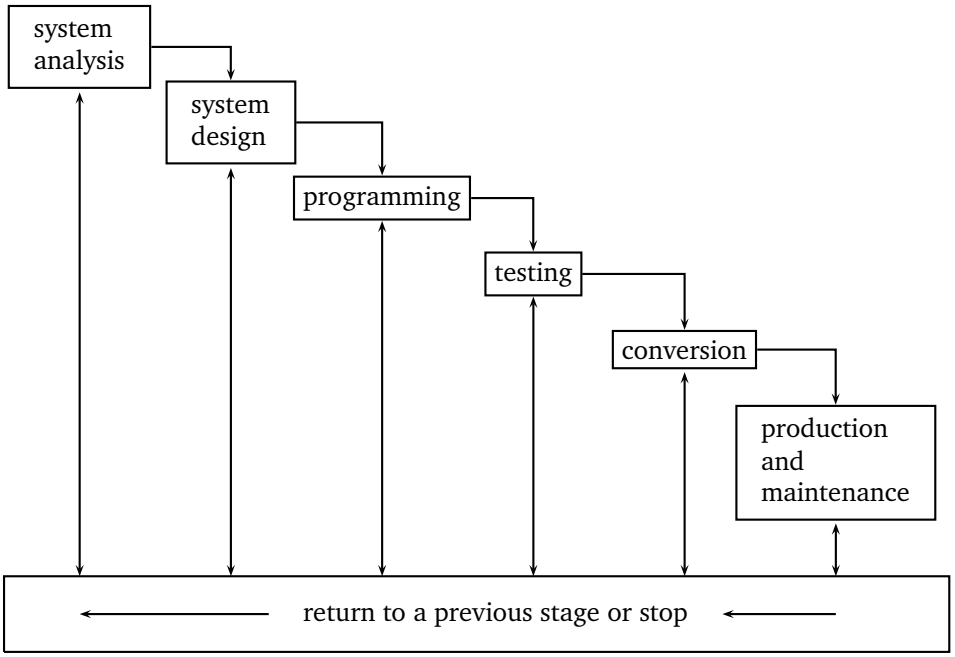


Figure 10.1: A six stage system development cycle

from making costly mistakes such as creating systems that will not work efficiently or that people will not use.

The systems analyst must also define the *information requirements* that must be met by the proposed system. Basically this means deciding who needs what information, where, when and how. Getting the information requirements wrong is a main cause of systems failure. Decisions that are made at this stage of the process are carried throughout the other stages so it is very important to get them right.

Finally the company should consider at this stage whether or not a new information system really is what they need. Would it be better to address their problems through a change of management or by providing more training?

10.4.2 System design

Systems analysis describes *what* the system must do and systems design describes *how* it is going to achieve this. The system designer produces a *system specification* that gives details of the following components and how they are going to be integrated:

- system outputs, inputs and user interfaces
- hardware, software, databases, telecommunications, personnel and procedures.

The system specification will determine how the new system will support the current organisational structure, or what changes in the current structure are necessary in order to successfully integrate the new system. The goal is to keep the system and the organisation in tandem – the organisation should decide what technology is

necessary and the capabilities of the system should help reshape the organisation.

There are two major aspects to system design.

- The **logical design** determines what the system will do, and how it will appear to users. It includes the design of outputs, inputs, processing, databases, telecommunications, controls and security.
- The **physical design** is the more technical side and determines how the system will actually perform its functions.

Another reason for the high failure rate of system development projects is that there is insufficient user involvement at the system design stage. Since end users have the capability to make the system functionless (if they refuse to use it) it is important to keep the end users involved and not let the logical design be over-ridden by the technical physical design.

10.4.3 Programming

Some companies may choose to use off the shelf software or fourth generation programming languages that enable the programming to be carried out by the end user (see section 10.5.4). Otherwise the programming phase of the development will probably be carried out by the company's IT department or outsourced to a company that specialises in developing custom application software. The programming should translate the specifications produced by the analysis and design stages into software program code – if not then a return to these stages is called for as a redesign might be required.

10.4.4 Testing

Thorough testing of every aspect of the system should be carried out to make sure that the system produces the right results. Testing is a time-consuming process and often not enough time is allowed for this stage. Testing might show up *bugs* in the program – either *syntax errors* (mistakes in the programming such as a missing semi-colon that stops the program from running properly) or *logical errors* (mistakes that mean that the wrong results are produced). In either case, the programmers have to go back and correct the error.

Different types of testing include:

- **Unit testing** – testing each part of the program in the system separately. This type of testing should be carried out continually as the program is developed.
- **System testing** – testing the functionality of the system as a whole to determine if the separate parts work together as expected.
- **Acceptance testing** – user and management evaluation of the system.

10.4.5 Conversion

Now that the new system has been designed, programmed and tested, it is time to actually start using it. There are different ways to implement a new system into the

company – none are right or wrong, which is best depends upon the system and the company.

- **Parallel strategy** – run both the old and the new systems at the same time until everyone is happy with the new system. This is the safest but also the most expensive approach.
- **Direct cutover strategy** – out with the old and in with the new. If the old system does not work anymore, or the company has total confidence in the new system then this strategy might be the best.
- **Pilot study strategy** – try the new system in a single area of the company and gradually increase its use if all goes well.
- **Phased approach** – this is similar to the pilot study strategy but the new system is introduced function by function rather than area by area.

Whichever conversion strategy is used, the users will need training and detailed documentation showing how the system works from both a technical and non-technical point of view. Lack of proper training is yet another reason for system failure.

10.4.6 Production and maintenance

The new system is said to be *in production* once the conversion is complete. It should now be reviewed by its users and designers to make sure that it has met its original objectives.

Continuing maintenance will be required to keep the system running smoothly and incorporate updates in hardware or software.

However good the system is, at some point it will become outdated and the whole process starts again.

10.5 Traditional and alternative methods for modelling and designing systems

Systems have traditionally been built in a very structured and orderly manner. Development teams consisting of systems analysts, programmers and technical specialists work through the *systems development life cycle* – the stages given in section 10.4.

The traditional method used to build a system is to start at the top and progress to the lowest detail. Processes that the system will carry out are thought of separately from the actual data that the system will process. *Data flow diagrams* are used to show how the data moves through the system. Using data flow diagrams helps the system designers track the progress of data through the system and see how different processes interact. Areas in the system that might cause problems, such as data incompatibility or bottle necks, can be spotted before the system is actually built.

Figure 13.5 on page 523 of Laudon and Laudon shows a simple data flow diagram for a University registration system. The round boxes represent three processes necessary to verify course availability, enrol the student, and confirm the

registration. The student is an external entity represented by a square box. The open boxes represent the data stores that will be required to carry out the processes file. The arrows represent flows of data and show the movement of the data around the system.

Learning activity

Consider an information system designed for booking appointments with a medical consultant. A patient requests an appointment, their details are confirmed, a time when the correct doctor is available is found, the patient is offered the appointment at this time.

Draw a data flow diagram that models this scenario. What external entities, processes and data stores does your diagram include?

Data flow diagrams can be used to show high-level processes or minute detail. A complex process, known as a *level 1 process*, can be broken down into a series of smaller processes and data flow diagrams can be drawn for each of these. These *level 2 processes* can in turn be broken down and so on until the lowest detail of level has been reached.

A *data dictionary* (see section 7.4.3) contains information about the individual pieces of data within the system. The data dictionary specifies the content of data flows and data stores. Using data flow diagrams with a data dictionary, it becomes possible to develop *process specifications* that describe how the data is going to be transformed into usable information. Hierarchical *structure charts* are top-down charts that show each level and how they interrelate.

This traditional systems development method is used for large projects such as developing an entire IT infrastructure. Such large and complex projects require rigorous and formal requirement analysis, predefined specifications and tight controls.

The disadvantage of using a traditional systems development life cycle approach is that generally one stage of the development is finished before the next starts and it can be very time and cost consuming to go back to previous stages. For many smaller systems which are less structured and more individualised this traditional life cycle approach might not be the most suitable.

In the following section we will consider some alternative approaches to system development.

10.5.1 Prototyping

The prototyping approach involves getting an initial list of user requirements, building a prototype system, getting user feedback and then redeveloping the system in response to the feedback and additional requirements. The steps of getting user feedback and further developing the prototype continue until the user(s) is satisfied that the system meets all of their requirements as shown in figure 10.2.

This approach can be faster and cheaper than the life cycle development approach and it is user centred. The user can guide the designer based on what they can see as the system is built. This means that the user is more likely to be happy with the end

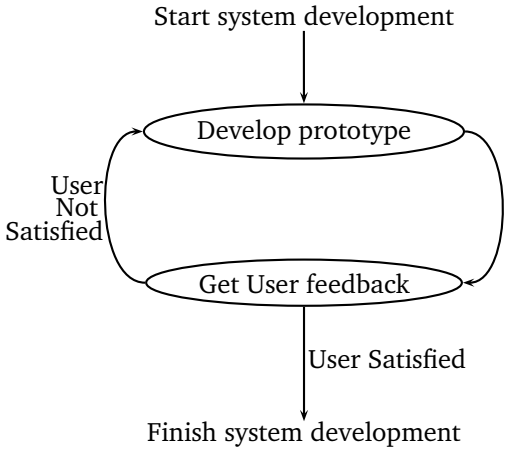


Figure 10.2: The prototyping approach goes through cycles of development and user feedback until the user is satisfied

result.

Prototyping is generally used for very small systems, or small parts of large systems. For example, for developing user interfaces and output reports – the areas that the user will see the most.

Prototyping would not be used to build a company-wide information system as it is too unstructured and difficult to manage for large projects.

10.5.2 Object oriented development

The traditional structured systems life cycle development method keeps data and processes separate. Object oriented development combines data and the processes that operate on that data and treats them as one entity called an *object*. Data which is encapsulated in an object can only be operated on by processes which are also associated with that object. In traditional programming, data is passed to a procedure. In object oriented programming, a message is passed for an object to perform an operation – the method used and the data required are already associated with the object. The whole system is modelled as a collection of objects and the relationships between them. If they are created correctly, objects can be re-used in different parts of the system.

Object oriented programming relies on the ideas of *class* and *inheritance*. Classes inherit features of their *superclass*. Figure 13.7 on page 526 of Laudon and Laudon shows how the classes *Salaried*, *Hourly* and *Temporary* inherit features of their superclass *Employee*. The different types of employee all have the features *id,name, address, dateHired* and *position* in common. However, the way in which their pay is calculated differs depending on which class the employee is in.

The advantages of object oriented development is that re-using existing objects reduces the time and cost of developing new software because it is not necessary to keep starting from scratch. Existing objects can be used as the building blocks for new applications. Systems built using the object oriented approach are more flexible because they can be modified and enhanced easily. Developing object oriented

systems means that the developers are forced to view the system in user terms rather than programming terms and this leads to more user friendly applications.

The disadvantage of object oriented development is that object oriented programs tend to run more slowly than those written in other programming languages. It may also be necessary to retrain the programming staff if they have little or no experience in using object oriented languages.

10.5.3 Computer aided software engineering (CASE)

So many things can be automated these days and software design and development is one of them. Computer aided software engineering (CASE) provides developers with an easy to use method of developing software code that is well documented, well designed and reusable. Software programs are generally becoming more and more complex with whole teams of programmers working on them and developing the code. CASE tools can be used to provide co-ordination and management for the programming team. They can also help to keep data flow diagrams and data dictionaries synchronised throughout the development.

The advantages of using CASE tools is that they generally bring more discipline and structure to the program design and development process. Systems produced using CASE tools usually have excellent documentation.

The disadvantages of using CASE tools to develop systems is that they are generally more expensive to build and maintain and require extensive and accurate definitions of user requirements. CASE tools can be difficult to customise and may be difficult to use to further develop existing systems.

10.5.4 End user development

For small projects, end user development might be a suitable approach. The end user takes matters into their own hands and designs and develops the system using a *fourth generation programming language*. The end user has complete control of the system, what it does and how it looks and so cannot blame anyone else if it does not meet their requirements. The tools available to assist with user development are getting easier to use but their capabilities are limited. Large and complex systems should not be built using this method. It can also be difficult to avoid problems with standardisation and there may be problems with compatibility between different parts of the system since each user will define their own way of doing things.

Table 13.3 on page 530 of Laudon and Laudon describes seven types of fourth generation tools:

- **PC software tools** such as *Microsoft Access*
- **Query languages** such as *SQL*
- **Report generators** such as *Crystal Reports*
- **Graphics languages** such as *SAS Graph*
- **Application generators** such as *QuickBase*
- **Application software packages** such as *Oracle PeopleSoft HCM*
- **High-level programming languages** such as *APL*.

The first of these are more likely to be used by end users, the last are more likely to be used by professional system developers.

Learning activity

For each of the seven types of fourth generation tools listed above, find an example (preferably a different example to the one given) of this type of tool and describe what it does and who is likely to use such a tool.

10.5.5 Rapid application development

Until a few years ago the time taken to develop a new information system was months or even years. These days that time frame has been shortened by some companies to days or weeks. Unfortunately the old saying "more haste, less speed" can sometimes be applied – doing things in too much of a hurry can lead to important steps such as proper testing being overlooked, and ultimately to the failure of the information system. That said, companies still want to reduce the time that it takes to develop an information system. *Rapid application development (RAD)* is used to describe the process of creating systems in a short time with technical specialists and end users working together using a variety of tools such as fourth generation programming languages, prototyping and automation to produce working systems.

Joint application design (JAD) is a technique used to get all of the technical specialists and end users together simultaneously to collect user requirements and create system designs. Getting everyone together at the same time will save time and hopefully lead to user agreement as to what the new system should do and look like. Of course it might be that the end users do not agree with each other at all, so a JAD meeting must be facilitated by a someone who is skilled in system design and analysis as well as people management so that they can resolve differences in a knowledgeable way.

10.5.6 Advantages and disadvantages of different development techniques

Table 10.1 summarises the different techniques for system development that we have discussed in this chapter and gives the potential advantages and disadvantages of each.

It may be that the company decides that it does not have the right people to carry out a system design or development in house. Or the company may decide to focus its efforts on its core business rather than using resources for software development. In this case the company may outsource the the work to an external company that specialises in system design and development.

Development Technique	Advantages	Disadvantages
Traditional System Development	Systematic and structured. Maintains standards by enforcing quality. Unlikely to miss important issues when collecting user requirements.	Excessive documentation. Users may be unwilling to engage, and be unable to describe their requirements. Time consuming to get from start of process to working system.
Prototyping	Users find it easier to clarify their requirements. The feasibility of the design is shown as the system develops. End users feel more involved with the process. Ill defined problems can be tackled.	Initial problem analysis may be inadequate. Best with only a small group of users. It may be hard to know when to stop development. Quality may be poorer if system is developed very quickly.
Object Oriented Development	Data and processes are integrated at the design and analysis stages leading to a high quality system. Common objects and classes can be reused making development and maintenance faster and easier.	Analysts and programmers may need to be retrained to use an object oriented approach. Object oriented programs usually run more slowly.
Computer Aided Software Engineering (CASE)	Bring discipline and structure to the development process. Produce excellent documentation.	Expensive. Require extensive and accurate user requirements. Might not be easy to integrate into existing systems.
End User development	The user controls the system so it should meet user requirements. IT staff are not involved and so can concentrate on other tasks.	Quality is lower with non professional programming. Documentation may be inadequate. IT staff may have to get involved to resolve problems. Systems may be inconsistent and incompatible.
Rapid Application Development (RAD)	Users are involved in design and so are more likely to accept the new system.	Building the system too quickly may result in poor quality.

Table 10.1: The advantages and disadvantages of system development techniques

10.6 Summary

In this chapter we have described the types of organisational change that can come about due to the introduction of new information systems. We have discussed the effects that these changes have and the importance of managing the people involved in system change as well as the hardware and software components of the system. We have described the traditional approach to software development using a six stage model. We have also looked at alternative approaches to system development including prototyping, object oriented development, CASE tools, end user development and rapid application development. We have compared these different methods that can be used to develop systems and discussed the advantages and disadvantages of each.

10.7 A reminder of your learning outcomes

After studying this chapter and the recommended reading you should be able to:

- describe the types of organisational change: automation, rationalisation of procedures, business process re-engineering and paradigm shifts, that may come about through the introduction of new information systems
- give examples of companies that have successfully gone through the process of business process re-engineering or paradigm shift
- explain why business process re-engineering fails in many cases and describe some of the reasons for the high failure rate using examples of companies whose attempts at BPR have failed
- explain the importance of quality management and the steps that companies can take to enhance the quality of their services and products
- describe the six stages (systems analysis, systems design, programming, testing, conversion, production and maintenance) of a traditional systems development life cycle
- describe alternative methods for developing an information system and discuss the advantages and disadvantages of each.

10.8 Chapter questions

1. Organisational change can range from automation to paradigm shifts. Explain why paradigm shift is the most radical form of change and why companies undertake such change even though it is so disruptive.
2. Describe some of the reasons why attempts at business process re-engineering fail.
3. Describe the six core activities that make up a traditional system development life cycle. Which of these do you think is the most important and why?
4. What are the advantages and disadvantages of using object-oriented development techniques instead of a traditional system development life cycle?
5. When would it be appropriate for a company to use an end user development approach to systems development?

Appendix A

Sample examination paper

Following is an examination paper from a previous year. The examination for this subject lasts for 3 hours. There are six questions on the examination paper and candidates are required to choose and answer any four questions. Calculators are not allowed. Marks available for each question part are given in [ ] brackets at the end of the question.

Solutions are given at the end.

A.1 Sample examination paper

2010 examination paper Zone A

Question 1

Scenario: Hotels for the Disabled

After forty years working as accountants, Mr Tom Davis and his wife Sue have both decided to change careers and open a chain of small hotels designed especially to cater for people who are disabled. Each hotel will have a member of staff for each room who will be responsible for ensuring the person staying in the room has all that they need.

Although they have not run a hotel before, Mr and Mrs Davis want the new hotels to be as technology-enabled as possible. They have read about the idea of having a digital firm and think if they can incorporate these ideas into their new business then they can make a profit.

One of the important aspects of the new chain of small hotels is that they have good communication systems and technologies. Each morning Mr Davis or his wife wants to be able to speak face to face with the manager at each hotel. Furthermore, in order to keep costs down, training of staff on issues concerning looking after disabled people will be done remotely wherever possible.

Mr and Mrs Davis believe that if they invest heavily in information systems they will be able to achieve significant improvements, not only in how they operate, but also how they interact with suppliers, make decisions and ultimately survive in a highly competitive market place.

As Mr and Mrs Davis are new to the hotel business it is also important that they learn from the data the business generates internally and from that which is available outside the business too. They want to purchase a system that will allow them to make use of the data they collect and turn that data into useful decision making and forecasting information.

For this question, you must use the information provided in the the scenario above.

(a) Describe how Mr and Mrs Davis can create a chain of hotels that can be described as a digital firm. Identify five of the major business relationships they would need to be technology enabled and describe the core business processes that would need to be accomplished through networks.[10]

(b) Explain why Mr and Mrs Davis believe they are right to consider investing heavily in information systems and describe five strategic business objectives that could be met by making this investment.[5]

(c) Recommend five communications technologies that Mr and Mrs Davis could invest in to insure the greatest level of communication between the different hotels in the chain. Make sure your recommendations include technologies to enable Mr Tom Davis or his wife to be able to speak face to face with the manager at each hotel every day and also train staff remotely.[5]

(d) Identify five kinds of data you think could be generated by Mr and Mrs Davis' business and describe the process of turning that data into useful decision making information. Also provide two recommendations as to what type of information system Mr and Mrs Davis should invest in and why.[5]

Question 2

(a) Mobile-Me is a company that manufactures mobile phones for several major retailers. Describe the main components of an information system Mobile-Me might use and detail six different environmental factors that Mobile-Me and its information system must interact with.[5]

(b) Using your knowledge of business such as Mobile-Me, compare and contrast the organisational dimension of information systems with the technical and behavioural dimensions of information systems used by business in this industry. For the organisational level provide examples of hierarchy of authority, separation of business functions, business processes and business culture and politics.[10]

(c) From a business perspective, information systems are part of a series of value-adding activities for acquiring, transforming, and distributing information that managers can use to improve decision making, enhance organisational performance, and, ultimately, increase firm profitability. Using your knowledge of businesses such as Mobile-Me describe the primary and secondary value-adding activities in a value chain associated with the manufacture of mobile phones and also the industry value chain for the mobile phone manufacturing industry.[10]

Question 3

Scenario: CarLand

Established in 1908, CarLand is the largest manufacturer of cars in Europe. Each one of CarLand's fifteen manufacturing plants has over fifteen thousand workers directly contributing to the design, manufacturing and distribution of new cars and lorries.

Although CarLand has very well organised production lines, it found that as it grew in size it was becoming less and less able to meet the demands from customers for customisations of cars on an individual basis.

One particular aspect of CarLand that was different from plant to plant was the set of business processes used to design, manufacture and then distribute cars. This was a problem in that staff and managers moving between plants had to learn whole new ways and processes for working.

Workers at CarLand also complained about either having too little or too much information. Furthermore, workers said that often the information they did receive was not at the right time and was not formatted correctly. As a result the information they did deceive was not appropriate and therefore could not be used for decision making. This was particularly true of middle managers. To compensate for this lack of timely and appropriate information, managers generally took to "over ordering" as a method of reducing the risk of running out of component parts or materials for cars that were being produced.

Some managers have now taken to creating their own small information systems, However, many of these systems did not communicate with each other. These islands of information were causing further problems as the data each held was often inaccurate.

For this question, you must use the information provided above in the scenario.

(a) Define and describe a set of business processes and related information systems that could be used by CarLand in the manufacturing of a new car. In your answer you must detail the relationship between the business processes and the information systems you recommend and explain the role played by the information systems in improving the efficiency of the business processes you defined.[10]

(b) To address CarLand's information problems, write a proposal for three new information systems that can address the needs of those working on the production line, middle management trying to make day to day decisions and those senior managers responsible for forecasting and planning. Explain why you have chosen a particular type of information system, what it will offer, and what benefits it will bring.[10]

(c) Describe in detail the three problems associated with different parts of the car plant having their own information systems and explain the problem of over ordering.[5]

Question 4

(a) Sitting Pretty is a chain of high street furniture shops that specialises in wooden tables and chairs. Furniture they sell comes from trees in Norway. Sitting Pretty is considering investing in a new information system to help them manage their relationship with suppliers. Describe the supply chain from source for one of Sitting Pretty's tables and explain how a supply chain management system can be used by Sitting Pretty to manage the firms relationship with suppliers. [10]

(b) Sitting Pretty is considering ways in which they can co-ordinate their business processes to increase customer service, get to know their customer needs better and increase customer satisfaction. Propose a type of information system they should consider using and describe how it would address the issues they wish to address.[5]

(c) Although Sitting Pretty has a website, it is very basic and was built several years ago by the owners' son. The website has no dynamic content and is merely the company's sales brochure. Sitting Pretty is planning to invest in a new Internet website as well as intranet and extranet sites for interacting with customers and suppliers. For each type of website propose three ways in which it can be used to provide Sitting Pretty's business.[10]

Question 5

Scenario: Government of Jatombee

The government of Jatombee has been debating and considering ways it can address its ever increasing crime rate. Since 1980 crime has gone up roughly 10% a year.

Although more and more police officers have been trained and a national campaign has been running to make people crime aware, both measures seem to be having little effect.

In 2005 Jatombee doubled the prison sentences for crimes of burglary, theft and violence. Although initially this measure did reduce crime levels they have began to creep up again.

At a recent meeting of the government it was suggested that technology could be the answer. The following proposals were put to the government as a way to solve the rising crime problem.

All members of the public would have a carry a signal emitting card that would broadcast their exact location at all times. Anyone caught outside without a card would be presumed to be a criminal or at least up to no good.

All people must only use the government approved email system which can be accessed and read by government bodies and private companies and individuals who present a compelling reason such as a job application or if they believe a person is committing a crime against them.

High definition cameras should be installed throughout the country, 150 yards apart. All cameras will be fitted with night sensors and infrared so that they can record people both in the day and at night.

All phone calls, texts, emails, video messages and other electronic communications would be recorded. This data would be submitted to a profiling and non-obvious relationship awareness system.

All web searches made would also be submitted to a profiling and non-obvious relationship awareness system.

All purchases made over 20 pounds sterling would have to made using a credit/debit card that would be linked directly to the national earnings, tax and insurance database. A persons' spending would be matched to their earning and if spending exceeded earning then a person would have to declare the reason why to the local police station.

For this question, you must use the information provided above in the scenario.

(a) The use of information systems to survey and control people raises major issues including information rights and obligations, property rights and obligations, accountability and control and quality of life. Describe five key technology trends that have enabled the government of Jatombee to feasibly consider implementing the proposals suggested.[5]

(b) Describe how the government of Jatombee could use the collected data via its monitoring of all phone calls, text, emails, video messages and other electronic communications as part of a Non-Obvious Relationship Awareness (NORA) information system to determine criminal behaviour.[5]

(c) Using the following five step process for ethical analysis, describe and explain the ethical dilemma raised by three of the proposals of the Government of Jatombee to reduce crime.[15]

Ethical analysis: A five-step process

(i) Identify and clearly describe the facts.

(ii) Define the conflict or dilemma and identify the higher-order values involved.

(iii) Identify the stakeholders.

(iv) Identify the options that you can reasonably take.

(v) Identify the potential consequences of your options.

Question 6

(a) Mr Stevens owns a bicycle repair shop in central London. Customers bring their bicycles to him for services, repairs and upgrading. Mr Stevens also sells second-hand bicycles to customers who want them. Until recently all administration concerned with servicing and selling of bicycles was done by Mr Stevens in paper based accounting books. This approach has worked well for many years. However with the recent rise in business such an approach to data management is no longer efficient or practical. A friend of Mr Stevens has suggested that he investigate the possibility of using a database management system for the shop. Mr Stevens has therefore hired you as a consultant to write the following short report.

Write a report of up to 500 words explaining how the problems of managing data using a traditional paper based file environment are solved by a relational database management system, Include in your answer a description of the capabilities and value of a database management system.[10]

(b) Using your knowledge of relational database management systems design, do the following:

(i) Create a database consisting of tables for bicycles, customers, bicycle parts, suppliers, service requests and parts to be serviced. Each table must have primary keys and be normalised to third normal form. [6]

(ii) Write an SQL statement to retrieve all the service requests for a customer called Jones.[3]

(iii) Write an SQL statement to retrieve the customer name and address and bicycle make and service request details for a customer called Evans.[3]

(iv) Write an SQL statement to retrieve just the customer name and the name of the bicycle make for every bicycle in the repair shop.[3]

A.2 Sample examination paper – solutions

Question 1

(a) The key difference between that of a traditional firm and that of a digital firm is that all major relationships are technology-enabled. Furthermore, all major business processes undertaken by the firm should be supported by appropriate technologies. A digital firm will seek to use information technology, people and systems, to provide it with a competitive advantage.

Although answers will vary, the following major relationships would be candidates to be technology enabled:

- the relationship between the hotel chain and its suppliers
- the relationship between the hotel chain and its customers wishing to book rooms in a hotel

- the relationship between different hotels within the chain for co-ordinating staff
- the relationship between the hotel chain owners and financial institutions
- the relationship between the hotel chain and their customers, once at the hotel
- the relationship between the hotel chain and those advertising and marketing the hotel chain
- the relationship between the hotel chain and its management and staff for co-ordinating and delivering training.

Three core business processes that would need to be accomplished using networks are:

- the booking of orders for hotel rooms and the taking of payments
- the management of the use of rooms and the use of special needs facilities by hotel guests
- the ordering and management of supplies of specialist equipment for guests.

Other relevant answers will also be considered.

(b) Mr and Mrs Davis are right to consider investing heavily in information systems because this will enable them to run their hotel chain efficiently and effectively. Information systems can be used to process important data so that key decisions can be made in an informed manner.

Although answers will vary, the five strategic business objectives that can be met through investing in information systems can include any of the following:

- Operational excellence through improvements in efficiency to obtain a higher profitability.
- Develop new products, services and business models for the hotel chain.
- Greater degrees of customer and supplier intimacy, leading them to understand customer and supplier needs, and thereby how best to serve these needs.
- Improved decision making through the ability to capture information and process this information: with more accurate data comes better decision-making.
- Competitive advantages gained will allow the delivery of better performance and reduced charging for superior performance. Information systems will also allow then to respond to customers' and suppliers' needs in real-time.
- The use of information systems by hotel chains can be viewed as a competitive necessity, and heavy investment in information systems will allow Mr and Mrs Davis to survive in a competitive market place.

(c) Although answers will vary, the following answers should be considered:

In an increasingly interconnected, networked world, jobs are becoming more interaction-based. They require systems that require workers to communicate, collaborate and share ideas. Such systems include:

- Internet-based collaboration environments such as Lotus Notes, Groove and Webex
- email and instant messaging
- cellphones and wireless handsets
- social networking tools
- video conferencing tools.

Adequate descriptions must be provided of how the five chosen communication tools can be used within the hotel environment.

(d) Although answers will vary, the following types of data could be generated by Mr and Mrs Davis' business, and should be considered:

- data concerning enquiries to stay at the hotels
- data concerning customer requirements
- data concerning how long customers want to stay at the hotel and what facilities they may use
- data concerning costs associated with running rooms at the hotels
- data concerning marketing costs per hotel room
- data concerning customer satisfaction surveys
- data concerning sales
- data concerning the analysis of specific marketing promotions
- data concerning numbers of visitors
- data concerning environmental context, i.e. current market cost of rooms, taxes, travel costs.

Mr and Mrs Davis need to invest in good transaction processing systems for each of the hotels. This will allow the day-to-day transactions such as booking customers into rooms and managing their stay at the hotels. Potential suggestions include:

- financial information systems, so all the accounting can be computerised and payments made electronically
- a customer-relationship management system to ensure the highest degree of customer-management intimacy and the highest possible chance of customer satisfaction
- a video conferencing system for day-to-day, face-to-face communication of all management staff and for training.

Question 2

(a) The main components of an information system that Mobile-Me might use are:

- input components
- processing components
- output components.

These interrelated components are used to collect, process and store distribution information. Mobile-Me will use them to support decision making, co-ordinating and controlling business processes. Inputting captures the raw data from internal or external sources. Processing converts this raw data into a meaningful form. Output transfers processed information to people to activities that use it. Feedback is output returned to appropriate members of the organisation to help evaluate or correct inputs.

Answers may vary, however environmental factors could include regulatory authorities, stockholders, competitors,m customer and suppliers.

(b) Although answers may vary, the following description can be used as an overall guideline.

The organisational dimensions of information systems include:

- the hierarchy of authority and responsibility, such as levels of management, i.e. senior, middle and operations, knowledge, data and production service workers
- separation of business functions, such as sales, marketing, human resources, finance and manufacturing
- unique business processes
- unique business culture
- organisational politics.

The technical dimensions of information systems highlight technological components such as:

- computer hardware and software
- data management technologies
- networking and communications technologies
- the information technology infrastructure that provides the platform upon which the information system is built.

A technical approach therefore emphasises the computer science, management and mathematics basis of information systems, whilst a behaviourist approach is much more interested in behavioural issues such as:

- strategic business integrations
- systems implementation
- resistance to change
- training and education.

From a behavioural perspective, the most important thing is how people use and interact with information systems, rather than the technology itself.

(c) A value chain is used to organise strategic business activities to design, produce, market, deliver and support products and services.

Primary activities are those directly involved in producing the final goods or services.

Secondary activities are needed to support primary activities, but do not directly have an input into the product or service provided.

Primary activities include:

- market research to identify customers for mobile phones
- computer aided design of various mobile phone handsets
- computer modelling of mobile phone contracts using spreadsheets
- purchasing of materials and supplies used in the manufacturing of mobile phones
- the manufacture of each mobile phone and the creation of each associated service plan
- the marketing and selling of mobile phones to customers
- the delivery of mobile phones and the provision of after-sales support.

Secondary activities include:

- human resources management
- component purchasing
- finance and accounting.

An industry value chain describes the large activities stream into which a particular business's value chain is embedded. It describes the processes that provide services to a particular business' value chain. The manufacture of a mobile phone can be described as follows:

(i) Mining companies dig up raw materials used to manufacture circuit boards.

(ii) Refining plant turns minerals into usable raw materials for the manufacturing process of mobile phones.

(iii) Factory assembles raw materials into printed circuit boards and then combines these with plastics and other internal components to assemble mobile phone devices.

(iv) Mobile phones are marketed and sold to shops and online outlets.

(v) Customer purchases and uses mobile phone.

(vi) Re-cycler disposes of old mobile phones.

Question 3

(a) Although answers may vary, the following set of business principles could be used to describe the design of a new car.

- Market research to identify a set of customer needs and functions from a new car. CarLand can use wireless handheld devices to interview members of the public about the design of future cars.
- 3-D models of potential designs for a car can be created, so that they can be evaluated efficiently and effectively. Computer Aided Design software can be used to create these 3-D models.
- Virtual models of how new designs will operate on the roads will need to be created and tested: simulation software can be used to perform these tests, and to generate data for feedback in the design process.
- Alternative designs for cars can be proposed so that popular designs can be pursued. An intranet system could be devised so that potential customers can review designs and provide feedback on them on the web.
- The cost of manipulating cars based on different designs will need to be known so that the manufacturing process can be costed. In this way, the total cost of producing different designs can be calculated. Spreadsheets could be used to create forecasting models of the total cost of creating new car designs.

(b) Information systems enhance business processes by increasing efficiency of existing processes, and enabling new processes that are capable of transforming a business. Often, technologies are used to change the flow of information, replace sequential steps with parallel steps, and eliminate delays in decision making.

A proposal for a new information system for those working on the production line at CarLand should be based on the need to support the many transactions that take place, as well as the operational level management that needs to be supported,

A materials requirement planning system is a transaction processing system designed to support the productions of products such as cars. It will allow operational management to know what components are required, which ones are in stock, and which ones need to be ordered. Furthermore, it will keep a record of components used on a daily basis in the manufacturing of cars.

Within CarLand, middle management is responsible for the overall manufacturing process and to provide senior management with good quality information for decision making. Middle management will therefore require a management information system which will provide them with reports on the activities of the production line and its workers.

A management information system will serve middle management by providing answers to routine questions such as what have we produced this week, how many orders are there left to fill and which orders are late?

A major responsibility of senior management is to make decisions and forecasts for future production. A decision-support system uses information provided by transaction processing systems and management information systems, to provide management with assistance in making non-routine decisions.

Decision support systems may be model- or data-driven and may be used to perform What If? analysis as well as providing help with current decisions.

(c) Although answers may vary, three potential problems associated with different parts of CarLand may include:

- update anomalies, in that different parts of the company could have different information held due to updating at different times
- duplication of effort, in that the same information could be stored several times in different places throughout CarLand
- it is difficult to enforce standards across different systems, especially in terms of interchangeability and interoperability
- over-ordering can lead to excess stockpiles, warehouse costs, and cashflow problems. Furthermore, the company is not benefiting from being able to keep its data in digital form for as long as possible.

Question 4

(a) Answers will vary, however, any supply chain should roughly take the following path:

- logger to saw mill
- saw mill to factory
- factory to distributors
- distributors to shops.

Supply chain management systems can be used to manage the relationships between all points in the supply chain.

Supply chains can also be used to ensure that products are kept in their design form for as long as possible, thereby enhancing the possibility for customisation.

(b) Although answers may vary, Sitting Pretty should consider utilising a customer relationship management system. Such a system could be used to:

- keep a track of customer orders and preferences
- provide support for products and services that exist
- mail-out recommendations for new product lines customers may be interested in
- understand customer needs through customer profiling
- increase customer satisfaction by answering queries promptly and satisfactorily
- collect customer data to fine-tune customer service-business processes.

(c) Although answers will vary, the following points are an indication of what should be raised under each type of system. An Internet system is a public website, available via a URL. Sitting Pretty could use such a system to:

- present products and services
- take customer orders
- provide background information on products sold
- provide company information and answer frequently asked questions
- allow customers to provide specified customisation on products they wish to buy
- perform e-commerce transactions, 24-hours a day, for customers around the world
- allow customers to contact the company for queries, sales and support.

An intranet website is a website only available within an organisation, and not available outside of it. It serves as an information resource, and method of interaction for those working within the company. Among other things, Sitting Pretty could use the intranet to:

- make available company forms such as invoices, ordering forms, customer satisfaction forms
- make available staff training documents, videos and audio files
- provide staff with an online forum for discussion and debate
- make available access to company wide information, such as customer details, price lists and stock levels
- host staff directories and make company announcements to staff.

An extranet is similar to an intranet in that it will make available company information, but its reach extends past that of direct employees to suppliers and possibly customers. Sitting Pretty could use an extranet to:

- inform customers of the progress of orders that they have made
- provide tailored support on products they have already purchased
- allow customers to inspect the source of products they are purchasing
- provide customers with extended information on products.

In addition, an extranet can be used by suppliers to:

- pre-empt orders by looking at stock levels
- provide information on their working practices
- demonstrate capacity used and where spare capacity may be available
- build higher relationships between Sitting Pretty and its customers so that each party has a greater understanding of each others processes.

Question 5

(a) Although answers may vary, the following key technology trends would enable the government of Jatombee to feasibly consider implementing the proposals suggested:

- ever-decreasing costs of hard disk storage capacity
- ever-increasing amounts of disk space availability
- miniaturisation of computing components
- the convergence of audio-visual computing components

- advanced data-mining technology and techniques
- decreasing costs of micro-processors
- wide-scale Internet working of computers and associated peripherals
- reductions in the costs of hardware and software components, such as webcams and network devices.

(b) Although answers will vary, non-obvious relationship technologies can be used by the government of Jatombee to take in information about people from disparate sources and find obscure, non-obvious relationships. For example:

- The government might use telephone records of a person wishing to be employed in a bank to deduce they share a house with a known criminal. This information could then be used to inform the hiring bank manager.
- The police could determine from text messages sent and when telephones are turned off, where a gang of criminals is about to commit a crime.
- By reading emails of the wife of a known criminal, and emails between the family members, the government might deduce where the proceeds of criminal activities are being secured.
- By interpreting video messages sent between family members, and phone calls made, it may be possible for the government to profile the kinds of people within a family who may wish to commit crime.

(c) Although answers will vary, the following is an example of how the email monitoring proposals of the Jatombee government raise ethical dilemmas and should be analysed ethically.

(i) Identify and clearly describe the facts:
The facts are that all people are required by law to use the government email system and allow government bodies, private companies, and individuals who can provide a relevant reason, to access emails.

(ii) Define the conflict or dilemma:
The conflict is between personal privacy and informing the public; between reducing choice so that monitoring can take place, and including the concept 'if you have nothing to hide then you have nothing to fear'.

(iii) Options: A,B,C:
A: Enforce the proposal in full, discounting any fears by saying it's for the good of the collective.
B: Operate a modified version of the proposal where a compelling reason must be presented by the police, private companies and individuals to an independent authority who will then decide how an individual's email can be read, and for how long.
C: Not enforce the proposal due to it being seen as an invasion of privacy.

(iv) Consequences of each action:
A: Implementation, support and management costs of introducing and running the system – financial costs of monitoring emails.
B: Cost issues including: delays in getting approval costs, costs when establishing the independent body and societal costs when approval is not granted to monitor a criminal's email.
C: Societal costs of the increasing levels in crime.

Provide answers to a further two dilemmas in a similar way.

Question 6

(a) Although answers will vary, the following provide examples of some of the problems of managing data, using a traditional paper-based filing system:

- difficult to search for data, as all searches must be done linearly
- difficult to delete unnecessary or unused data as it can only be crossed out
- difficult to do updates on data because it has to be crossed out and written over
- difficult to update the same piece of data across different records
- difficult to insert data into an existing paper-based filing system
- difficult to query data
- difficult to make relationships between data held in different paper-based filing systems
- difficult to analyse the data held, it would need to be inputted into another system
- difficult to sort data in other ways other than the system it was originally written and filed in.

A relational data-based management system consists of data held in tables. Each table is made of a collection of records, one for each instance of an item stored in the table.

A record is made up of a collection of fields. Each is used to store an attribute value for the instance. Individual records are identified using keys.

A key may be a candidate key, made up of a combination of attribute values that uniquely identify a record, or a primary key, which itself uniquely identifies the record.

Records are located using a Structured Querying Language (SQL). Tables can be joined by matching primary keys, with instances of them in other tables, where they are referred to as foreign keys.

Using relational data-based tables and SQL, many of the problems associated with paper-based systems can be solved. For example:

- easy to sort tables based on attribute values held in field
- easy to insert new records into a data-based table
- using SQL, one or more records can be selected, and then easily updated or deleted
- data can be exported from relational data-based tables into analysis programs
- management reports based on SQL queries can be created easily.

(b) (i) Bicycles: id, customer_id, name, company_name.
Customers: id, name, address1, address2, postcode, phone_number, email_address.
Bicycle_Parts: id, name, supplier_id, cost.
Suppliers: id, name, address1, address2, postcode, phone_number, email_address.
Service_Requests: id, customer_id, bicycle_id, service_date, service_completion_date.
Parts_to_be_serviced: Service_request_id, bicycle_part_id.

SQL statements for parts (ii) to (iv) will vary but following are example solutions which use the table and column names given in part (i).

(ii)
```
SELECT*
FROM Service_Requests
WHERE customer_id=(SELECT id FROM Customers WHERE
name=”Jones”);
```
or
```
SELECT s.* FROM Service_requests AS s, Customers AS c
WHERE c.id=s.customer_id
AND c.name=”Jones”;
```

(iii)
```
SELECT c.name, c.address1, c.address2, c.postcode, b.name, s.*
FROM Bicycles AS b, Customers AS c, Service_Requests AS s
WHERE b.customer_id=c.id
AND s.customer_id=c.id
AND c.name=”Evans”;
```
or
```
SELECT c.name, c.address1, c.address2, c.postcode, b.name, s.*
FROM Bicycles AS b
JOIN Customers AS c
ON b.customer_id=c.id
JOIN Service_Requests AS s
ON s.customer_id=c.id
WHERE c.name=”Evans”;
```

(iv)
```
SELECT c.name AS “Customer Name”, b.name AS “Bicycle Name”
FROM Bicycles AS b
JOIN Customers AS c
ON b.customer_id=c.id
```
or
```
SELECT c.name AS “Customer Name”, b.name AS “Bicycle Name”
FROM Bicycles AS b, Customers AS c
WHERE b.customer_id=c.id
```

Appendix B

Solutions

B.1 Solutions to Chapter 6 Questions

1. Answers will obviously vary but should include references to hardware costs, including cabling, telephone line access charges, and printer costs such as paper and ink cartridges; software costs, including programs, licences, upgrades and fixes; human costs such as training and technical support including salaries.
2. Five drivers of the IT infrastructure evolution include:
   - Moore's Law – the number of components on a chip with the smallest manufacturing costs has doubled approximately every 18 months – this is exponential growth.
   - Digital storage – the amount of digital information is roughly doubling every year and the cost of storing digital information is falling exponentially.
   - Metcalfe's Law – the value or power of a network grows exponentially as a function of the number of network members. The benefits of adding a new person to an existing network greatly outweighs the expense.
   - Declining communication costs – the rapid growth of the Internet is in part due to declining communication costs meaning that more and more people are able to get online.
   - Improved standards – specifications that establish the compatibility of products and their ability to communicate with each other make the Internet a more useful and user-friendly environment in which to conduct business.
3. Cloud computing allows an organisation to purchase computing capacity from remote, large-scale data processing centres during periods of peak demand. The organisation only needs to purchase the capacity or service that it needs at any given time, thereby providing a scalable IT solution. Companies offering the cloud computing services can provide other organisations with new technologies that they might not be able to provide for themselves.
4. Java is a computer programming language which uses applets that are miniature programs which perform very small, specialised, one-at-a-time tasks. The code needed for the required applet is run on the client computer and when the task is completed it is discarded. This reduces the need for storage on the client computer and means that Java applets can be used on small handheld computers and other appliances such as mobile phones. When using Java, people do not have to purchase and use huge software programs. Java fulfils the need for interactive programming over the Internet. It is both operating system and processor independent.
5. Open-source software provides business value by lowering the cost of purchasing software because open-source software is free to download and use. Open-source software is generally superior to commercial software because thousands of programmers around the world work (for free) to read, test, modify, perfect and distribute the code. These sorts of resources (thousands of programmers) are not available to commercial software companies.

B.2 Solutions to Chapter 7 Questions

1. Problems associated with managing data in a traditional file environment include:
   - islands of information
   - data redundancy
   - data inconsistency
   - program-data dependency
   - lack of flexibility
   - poor security
   - lack of data share and availability.

   A database management system stores all of the information in a centralised database which reduces islands of information. The data in the database is constructed separately from the programs that will use it and the formats into the appropriate form depending on which application is requesting it. This solves the problem of program-data dependency. As all the data is stored in one place, it is easier to find instances of data redundancy, and eliminating these reduces the problem of data inconsistency. The DBMS resolves the problems of lack of flexibility, lack of data share and availability because it can present whatever data is required regardless of the fact that the data may be stored in multiple tables and in different formats. As there is only one database rather than multiple file systems, it is easier to keep the data secure.
2. A relational database management system works by storing the data in a set of tables. Each table stores records of entities and their attributes and includes a primary key field which uniquely identifies each entity. Data from two different tables can be merged by storing the primary key from one table as the foreign key in the second table and vice versa. Now there is a relation between the two tables. Using a relational DBMS it is possible to select, join and project data to form whichever tables of information are required. A relational DBMS is a very powerful tool in terms of turning data into information because of its great flexibility and the ease of accessing data that it provides.
3. Web browsers are easier to use than most database query languages for accessing and compiling information. An organisation can build a web-based *front end* to the database without the need to rework the structure of the actual database. No special software is required for users and they not likely to need a lot of training in order to use the browser to access information from the database.
4. It is very important to involve the end users (people from different departments for example) when designing a database. Even though a department may not be connected to the database initially it is likely to be at some point in the future. The technical specialists who design and implement the database may have very different ideas about what is important from the end users and it is very important that they talk to each other at every step of the design. If this is not done it may be that the database is not user friendly and does not provide useful information. External end users should also be involved (for example through using a trial group) as it is important that external users have a good impression about the company and this could be destroyed if they find the database unhelpful or difficult to use.
5. You could describe any three of:
   - data warehouses

- business intelligence
- online analytical processing
- data mining
- using a database server and application server to access database information in the form of web pages.

B.3 Solutions to Chapter 8 Questions

1. The Transmission Control Protocol and Internet Protocol (TCP/IP) provide a universally agreed method for breaking digital messages up into packets, routing them to the correct address and then reassembling them back into the original message. Businesses using the TCP/IP standard can use a wide variety of hardware and software without the need to create proprietary software and special hardware. The universal acceptance of TCP/IP means that businesses can build networks that anyone/anywhere can use.
2. Internet services that are available to businesses include e-mail, instant messaging, wikis, discussion forums and newsgroups, telnet and FTP, virtual private networks, VoIP and the web. Describe any of these – see section 8.6.3. All of these services provide a universal method of connecting employees, customers, suppliers, and business partners in a fast and inexpensive way.
3. Voice over Internet Protocol (VoIP) enables businesses to use Internet technology to make telephone calls over the Internet or a private network. VoIP technology uses the Internet Protocol (IP) to deliver voice information in a digital form using packet switching. This avoids the high cost of making long distance telephone calls on a traditional telephone network. VoIP calls can be made from any computer connected to the Internet if it is equipped with a microphone and speakers.
4. Answers will vary but should include information about the benefits of linking functional areas of the work or learning environment under discussion. The aim of this is to increase communication between different colleagues and teams (or between students and teachers and other staff). The benefit of this is that information is more accessible and the costs associated with disseminating information are reduced. You should address the problems of how to integrate wireless technology into the existing IT infrastructure, how to maintain security and privacy, and how existing business/learning relationships may change.
5. The terms the *Internet* and the *world wide web* or *the web* are often used interchangeably. This is not strictly correct because the Internet is a huge network of computers with a client/server architecture. The world wide web is a set of interconnected documents which are contained on the Internet. You can think of the Internet as hardware and the world wide web as software.

B.4 Solutions to Chapter 9 Questions

1. Wireless networks are built to allow computing devices to easily connect with each other and transfer data and this makes them susceptible to hackers listening in. The service set identifiers (SSID) which identify access points in a Wi-Fi network are broadcast multiple times. This means that they can be easily picked up by hackers using sniffer programs – the hackers can then gain access to other devices on the network. Hackers might also establish rogue access

points at Wi-Fi hotspots and capture the username and password of genuine users. Companies can protect their wireless networks by using Wired Equivalent Protection (WEP) and by encrypting any sensitive data that is to be transmitted over the network.

2. A denial of service attack is when an information system is flooded with requests and crashes. The multiple requests might come from a *zombie network* of computers that have been infected with a worm or virus. Genuine users are unable to access the system which can have an enormous impact on the company or organisation whose system is under attack. Specific examples of denial of service attacks will vary according to the company chosen. It is hard to prevent denial of service attacks because the requests that flood the system are the same as genuine requests which the company would not want to prevent. However the company could use a method that makes sure that it is a genuine person rather than a computer making the request such as forcing the user to copy a series of random distorted letters from the screen. The company could also have a back up system in place if a risk assessment shows that a denial of service attack would have such a detrimental effect that this is a good use of resources.

3. Employees are the biggest threat to information security either by intent or by accident. Employees already have access rights to information systems and if they choose to abuse those rights it is hard for the company to stop them. Instead the company should have good audit trails and accountability so that they can pinpoint any wrong doing to the perpetrator. Apart from malicious intent, employees can risk the security of their company's information systems and the data held on them through negligence or stupidity. Employees might use weak passwords or reveal their passwords. They are also more likely to access dubious websites or open suspicious attachments at work rather than at home because they think that the companies firewall and anti-virus software will protect them and that the IT staff will be able to resolve any problems that result from their actions. Training the workforce in computer security and enforcing a good security policy are of paramount importance in the fight against computer crime.

4. If your car has been stolen it is not hard to realise this fact – the car is physically missing. If a secret recipe is stolen then you might not be aware of this because the thief will have copied the recipe but also left the electronic copy on the computer. You can deter car thieves by using a car alarm, locking the car and parking it in a secure place. You can deter computer criminals by using access controls and encryption. The police will look for physical clues when hunting for car thieves – the police wherever the car is stolen will be the ones to investigate the theft. There are unlikely to be any physical clues when hunting for computer criminals and the crime may have taken place miles away from the computer from which the recipe was stolen.

5. A good security policy should cover acceptable use, user authorisation and authorisation management systems. The policy should include statements ranking information risks, identify acceptable security goals, and identify mechanisms for achieving those goals. The policy should also describe who generates and controls information, what existing security policies are in place to protect information, what level of risk the management is willing to accept for each asset, and estimates of how much is will cost to achieve an acceptable level of risk.

B.5 Solutions to Chapter 10 Questions

1. Paradigm shifts are the most radical because they require the company to rethink the very nature of their business and the necessity for moving into whole new markets. Paradigm shifts can cause major disruptions and extreme change throughout the entire organisation. However companies must undergo these changes in order to stay competitive. They have to cut their costs and streamline their operations due to global economic pressures and changes to the industry brought about by external influences such as the Internet.
2. Business process re-engineering attempts fail due to the high cost and time commitments that they take to implement. Companies often fail to plan adequately for the changes that their employees and customers will experience. Lack of communication can lead to people being unwilling or unable to work with the new system leading to system failure.
3. The six core activities that make up a traditional system development life cycle are systems analysis, systems design, programming, testing, conversion, production and maintenance. See section 10.4 for a description of each of these. All of these stages are important and failing to do any of them properly can lead to system failure. You could argue the case for any one of them being the most important.
4. Object oriented development combines data and processes into single objects that become the basic unit of systems analysis and design. This leads to high quality systems. Object oriented development reduces costs and time because objects are reusable as building blocks for other systems. However programmers and system developers may need retraining in order to work with object oriented programming languages, and object oriented programs tend to run more slowly than traditional software programs.
5. A company might use an end user development approach to developing a new system if the system was only a small part of an overall infrastructure; the end user in question was confident in how to use fourth generation programming languages and query languages; the new system did not have to interact with other parts of the system so that data incompatibly or inconsistency of output reports or input/output functions will not cause a problem.

Index