Heriot-Watt University Study Guide

BSc Information Technology
Professional Development

Interactive University

Edinburgh EH12 9QQ, United Kingdom.

First published 2005 by Heriot-Watt University

Copyright © 2006 Heriot-Watt University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without written permission from the publisher.

Heriot-Watt University accepts no responsibility or liability whatsoever with regard to the information contained in this study guide.

British Library Cataloguing in Publication Data

Interactive University

Heriot-Watt University Study Guide: Professional Development

1. BScIT I. Professional Development

Typeset by: Interactive University, Wallace House, 1 Lochside Avenue, Edinburgh, EH12 9QQ.

Printed and bound in Great Britain by Graphic and Printing Services, Heriot-Watt University, Edinburgh.

Part Number 2006-1483

Contents

Topic 1

Professionalism

Contents

Learning Objectives

- *Awareness of the role of a professional in society*
- *Appreciation of the importance of competence, responsibility and trust*
- *Awareness of the role of a professional body*
- *Familiarity with the codes of conduct and practice governing the IT profession*

This project is of 25 weeks duration. There are milestones in terms of project submissions at weeks 6, 12 and 18.

Please refer to the Student Guide to Plagiarism before you complete and submit your coursework.

1.1 Introduction to the Unit

"The time has come," the Walrus said,
"To talk of many things:
Of shoes - and ships - and sealing wax -
Of cabbages - and kings -
And why the sea is boiling hot -
And whether pigs have wings."

(Lewis Carroll, 1872)

In this unit we shall investigate many issues - ranging from the technological, to the sociological. We shall discover that modern society is heavily dependent on Information Technology and that it lays down laws and regulations to constrain and control that dependence. Some of these rules can only be complied with through the introduction of further technological solutions, such as the security measures necessary to protect the privacy of personal data.

One of the most important outcomes of these investigations is to ensure that you know how to adopt a professional attitude towards the application of information technology. In order to assist you in this we shall first examine what it means to be a professional and what constitutes a "profession". We shall look at the kinds of codes, standards and laws that are likely to guide and govern your actions and we shall cover methods you might find useful when making ethical decisions.

The risks and threats that arise from the use of information technology are not always easily foreseen. You will discover, however, that society expects its information technology professionals not only to be more aware of these risks and threats than anybody else but also to have solutions ready to hand when they manifest themselves. This is a pretty tall order and sometimes the best you will be able to do is to provide an acceptable explanation for why you couldn't foresee, or cannot deal with, a particular event. In this unit we shall help you to distinguish those explanations which are likely to be acceptable from those which would definitely be unacceptable. We shall look at the kinds of crime which can be perpetrated by and on computers and some of the security measures which can be used to combat them and maintain the integrity and confidentiality of data.

The growing use of computers in safety-critical systems is perhaps the most obvious example of society's dependence on information technology but there are many, seemingly less important dependencies, which can have profound effects on our lives when things go wrong. We shall look at some of these and also at the way in which societal attitudes can influence the speed and direction in which technology develops, for the better but also for the worse.

Finally, we shall look to the future and, whilst not being so foolish as to try to make predictions, we shall look at current trends in computing and communications technology and consider where they might be leading us.

There is no single book which covers all of the material in this unit but "Ethics for the Information Age" by Michael Quinn comes closest. It is recommended that you read a computing industry newspaper or magazine on a regular basis. At the end of each topic references to supporting material will be provided and you should dip into these as and when a particular subject attracts your interest.

1.2 What is a professional?

This seems like a pretty straight-forward question, doesn't it? We've all met professionals - doctors, lawyers, etc. But what is it that makes them professionals? Is it their standing in the community? The fact that we tend to hold them in high regard? Surely, that is a consequence of their being professionals rather than the reason for it? Their expertise plays a large part in it of course but that cannot be the whole story for there are many people with highly specialist expertise who are not regarded as professionals.

1.2.1 Competence-Responsibility-Trust

We expect technical competence from a professional. They should be well trained and experienced in their art. Being a professional means knowing what to do and keeping up to date with the latest developments and methods. This is referred to as Continuing Professional Development and generally runs throughout a professional's career.

We also expect a certain level of responsibility from professionals. Responsibility for their work and their actions. Responsibility to, and for, their patients and clients. They should also be responsible enough to know their own limitations and not attempt tasks which they know they cannot undertake successfully. Being a professional means knowing when to refer a matter to others, just as a general practitioner in medicine knows when to call in a specialist consultant. We expect professionals to act in our best interests even, indeed especially, when we don't know what they are ourselves.

Possibly more than anything else we expect trustworthiness from a professional. When a lay person consults a professional, they are doing so because they know they do not have the knowledge or understanding to solve their problem themselves. By definition then, they do not have the knowledge or understanding to assess the wisdom or correctness of the advice or actions of the professional. They must trust the professional. They have no choice but to do this. Furthermore, in making use of the services of a professional, it is often necessary to disclose confidential information and the relationship of trust is therefore critical in the relationship between a professional and their patient or client.

Perhaps you can think of other factors which play a part in defining those whom we regard as professionals. Feel free to add them to the list but Competence, Responsibility and Trust (CRT) must surely remain at the top.

1.2.2 When do you become a professional?

The simple answer to this question is that you become a professional when people treat you as if you are one and you respond professionally. Perhaps you already are a professional. When a friend or relative asks you for advice on a computing matter, if you act responsibly and only give advice on matters which you know you are competent to handle and if you refer people to appropriate sources or services on matters which you aren't competent to handle and if, in any event, you respect any confidences that might have been imparted to you, then you are a professional.

You cannot provide any certificates or guarantees of your professionalism though. So how can somebody who doesn't know you decide whether they can trust you? Wouldn't it be better if there was some certificate or other document which you could show people through which they could be assured that you have been checked out and your competence, responsibility and trust can be vouched for.

1.3 What is a profession?

A profession is, quite simply, an occupation in which the practitioners are overseen by a professional body. Membership of professional bodies is often voluntary but in some cases it can be against the law to practise if you aren't a member of the relevant professional body. This is nearly always the case in the legal and medical professions and not uncommon in particularly critical types of engineering. Professional bodies can impose sanctions on members who do not abide by their guidelines or who behave improperly. Doctors can be "struck off" if their governing professional body decides that their poor performance or behaviour means it is not in their patients' interests for them to continue to practise.

1.3.1 Guarantor of C-R-T

A professional body is the guarantor of a practitioner's competence, responsibility and trust. In the final analysis, it is the existence of a professional body that turns an occupation into a profession and its practitioners into professionals. Membership of a professional body is the proof that a particular practitioner abides by certain codes of conduct and practice, that they are suitably qualified and experienced and that they can be trusted. The certificate that assures the general public that a person is a professional is their membership certificate of the appropriate professional body.

1.3.2 The British Computer Society

The British Computer Society (BCS), founded in 1957, is the professional body for Information Technology professionals in the UK. With over 47,000 members in over 100 countries around the world, the BCS claims to be the leading professional and learned society in the field of computers and information systems. In addition to their own professional examinations of competence in the various branches of computing, the BCS also accredit courses run by others as meeting the BCS academic requirements for membership. The BCS runs a Contining Professional Development programme through which it seeks to ensure that its members remain in touch with the latest developments and ideas throughout their careers.

Student membership of the BCS is relatively inexpensive and can offer many benefits. You should visit the BCS website to see what it has to offer. Amongst other things on the site, you will find their "Code of Conduct" and "Code of Good Practice".

1.4 Assigned task

Familiarise yourself with the British Computer Society's "Code of Conduct" and "Code of Good Practice".

The BCS Code of Conduct can be found at http://www.bcs.org/BCS/AboutBCS/codes/conduct/

The BCS Code of Good Practice can be found at http://www.bcs.org/BCS/AboutBCS/codes/cop/

1.5 Assessment

End of topic test

Q1: Which of the following should not guide a professional's actions?

a) Codes
b) Laws
c) Publicity
d) Standards

Q2: Which of the following was not recommended as supporting material for the Unit?

a) "Ethics for the Information Age"
b) Industry advertisements
c) Industry magazines
d) Industry newspapers

Q3: Which of the following would you not regard as a professional?

a) Doctor
b) Engineer
c) Lawyer
d) Plumber

Q4: What does C-R-T stand for?

a) Cathode Ray Tube
b) Competence-Reliability-Trust
c) Competence-Responsibility-Trust
d) Cuticle Replacement Therapy

Q5: Which of the following is not required of a member of a professional body?

a) Abiding by a code of conduct
b) Earning lots of money
c) Qualifications
d) Trustworthiness

Q6: Which of the following was not cited as an indication that you are a professional?

a) Behaving as if you are
b) Being treated as if you are
c) Believing you are
d) Respecting confidences

Q7: In which year was the British Computer Society founded?

a) 1956
b) 1957
c) 1970
d) 1984

Q8: In which UK city are the headquarters of the British Computer Society?

a) Birmingham
b) Edinburgh
c) London
d) Swindon

Q9: Which of the following is not a section in the BCS Code of Good Practice?

a) Practices common to all disciplines
b) Key IT practices
c) Practices specific to industrial functions
d) Practices specific to business functions

Q10: Which of the following is not a section in the BCS Code of Conduct?

a) Giving value for money
b) Duty to the profession
c) The public interest
d) Professional competence and integrity

1.6 References

British Computer Society, 2005, *Welcome to the British Computer Society* [online]. 2005 [cited 10th July 2005]. HTML. Available from http://www.bcs.org/bcs

Carroll, L., 1872, *Through the Looking Glass and What Alice Found There*, in *The Penguin Complete Lewis Carroll*, Harmondsworth, 1982.

Quinn, M.J., 2005, *Ethics for the Information Age*, Addison Wesley.

Topic 2

Rights and Wrongs

Contents

Learning Objectives

- *Awareness of the international codes and standards governing the profession*
- *Appreciation of the law as it relates to computing*
- *Understanding of methods for the rational resolution of ethical problems*

2.1 Introduction

A variety of instruments can be used to identify which practices are regarded as acceptable and which unacceptable. Depending on whether these instruments are framed as professional codes, industry standards or statute laws, the punitive measures for malpractice can vary considerably in their severity. In this topic we shall look at the ways in which the computing profession can be regulated.

Rules and regulations aside though, we all bring our own moral values and ethical principles to bear when considering the rights and wrongs of a particular course of action. When our values and principles form a major part of the justification for our actions it becomes imperative that we are able to articulate them clearly to others. This can be very difficult if we are not used to doing so though. We shall examine methods which can assist us in applying our ethical standards and explaining them to others.

2.2 Codes and standards

Compliance with codes or standards is generally voluntary, rather than compulsory. Professional codes are accepted voluntarily when one joins a professional body and failure to comply with the codes will normally result in expulsion from the professional body at worst. Industry standards are guidelines which should be followed, and might be a requirement for membership of certain industry associations, but they are not obligatory.

2.2.1 Codes

All professional bodies have codes of conduct and/or practice. We examined the codes of the British Computer Society in the previous topic. Other codes with which you might already be acquainted include the Code of Ethics and Professional Conduct of the Association for Computing Machinery (ACM) and the Software Engineering Code of Ethics and Professional Practice of the Institute for Electrical and Electronics Engineers Computer Society (IEEE-CS) jointly with the ACM (Quinn 2005). Intellect promulgate an IT Supplier Code of Best Practice and even the International Standards Organisation (ISO) has a Code of Ethics.

The emphasis on professional bodies and the sanctions which they can impose on members who do not comply with their codes does not mean that non-members are in some way exempt from these codes. Because the bodies are recognised as representing their professions and work hard to publicise their codes, no practitioner can credibly claim ignorance of them, nor be forgiven because they happened not to be member. Familiarity and compliance with these professional codes of conduct and practice is expected of all practitioners, whether members of the professional body or not.

Typically professional codes will require that the practitioner pays due heed to -

- Staying up to date in knowledge of their craft
- Developing the knowledge and careers of others for whom they are responsible

- Providing clients with the most appropriate solutions to their problems
- Providing clients with impartial advice
- The interests of the public as a whole

That last bullet point can cause more heart-ache and lost sleep than all of the others combined. It places a requirement on the practitioner to look at the bigger picture surrounding what they are doing and the possible side-effects of their actions or recommendations. Doing the best job one can for a client is relatively straight-forward but it is not always the case that what is best for a particular client is best for society at large.

2.2.2 Standards

Standards organisations lay down guidelines for all sorts of manufactures and services. It is expected that a practitioner will be aware of and comply with any national and international standards pertinent to their work. Whilst the standards themselves are not enshrined in law they can play an important part in legal cases. A defence against a law suit for negligence, for instance, is unlikely to be upheld if the relevant standards have not been complied with in the work of the defendant.

Of greatest importance are those standards that have risen to international status. The International Standards Organisation (ISO) publishes a number of standards relevant to the IT profession. Two with which you should familiarise yourself are -

- ISO 9000 Quality Management and Quality Assurance
- ISO 17799 Information Security Management Systems

The former actually has a computerised certification process known as TickIT which was especially developed to assist the computer industry in becoming compliant. It s worth noting, however, that even international standards are not beyond criticism. ISO 9000 is a case in point here, for it has been roundly accused of inflexibility and consequently actually reducing quality in some circumstances (Seddon, 1997). Having said that, it would be a foolish person indeed who tried to use Seddon's arguments as a reason for not using ISO 9000 if they didn't employ any other quality management system instead.

2.3 Computer law

Compliance with statute laws is, of course, mandatory and failure to comply can result in fines or imprisonment. There will probably be many laws within the jurisdiction where you live or work that are relevant to the IT profession. Some will be applicable to a wide range of activities with no special treatment given to computing. Some will pre-date key developments in computer technology and might have been amended (possibly in an unsatisfactory way) to cope with these developments as they arose. Others will have been framed specifically to deal with issues which result from computer and communications technology.

In the following sections we shall briefly examine five broad categories of laws that impact on the IT practitioner. You should not expect to be able to handle your own legal affairs as a result of the instruction you receive on this course but it is important that you are able to recognise situations when you need to call upon the services of a professional lawyer.

2.3.1 Contracts and consumer protection

Contracts, torts (wrongs) and restitution form a class of laws which generally have a long history and are unlikely to make special reference to the IT industry. You should note, however, that contracts can sometimes be held to be unfair and therefore not binding on the signatories. Indemnity clauses, where a contract states that the supplier cannot be held responsible for death or injury resulting from their product or service, are most likely to fall into this category. Consumer law can also be brought to bear in cases where fitness for purpose or safety are called into question. Compensation payments when things go wrong can be enormous. You should always take the advice of a lawyer when drawing up or signing a contract.

2.3.2 Intellectual property

Intellectual Property Rights (IPR) have become a hot topic with the development of IT and the Internet. With two notable exceptions, there is really nothing special about the computing industry when considering IPR; computer hardware can be protected by patents like any other invention and computer software can be protected by copyright like any other recorded form of intellectual property. In some jurisdictions changes were required to legislation to cater for electronic, as opposed to printed, forms but that was a relatively simple amendment to make.

The reason IPR has become such a hot topic, of course, is that computer and communications technology make it so easy to copy other people’s work and so difficult to identify where that copying has actually taken place. It’s not the case that laws need to be changed, it’s that they have become so difficult to enforce. From the point of view of the IT profession, the main concern is to ensure that reasonable measures are taken to protect the IPR of others - the IPR of IT developers doesn’t require any special new laws to protect it.

But what of the two notable exceptions we mentioned earlier? Well, one concerns computer algorithms and the other relates to the "look and feel" of computer programs and they cause problems because there is no consensus on how to handle them.

For computer algorithms the controversy arises over whether they should be patentable. It is not possible to copyright a computer algorithm. On this there is consensus. It is possible to copyright a particular implementation of an algorithm - as long as there is scope for a diversity of such implementations - but the idea of the algorithm, its essence, is not appropriate for copyright protection. If a computer algorithm is regarded as an "invention", however, then it should be possible to protect it with a patent. On the other hand, if an algorithm is viewed as a mathematical method then it should be treated like any other "discoverable" thing and thus be excluded from being patented. The argument rages on, particularly between the USA, which takes the former view, and the European Union, which takes the latter. Both sides claim that their approach offers the greater benefits to society as a whole. You might like to try listing their respective benefits for yourself.

The issue of the "look and feel" of computer programs boils down to whether we need a new kind of intellectual property. Suppose you create a computer program with a particular screen display and a particular layout of buttons, menus, etc. Suppose now that somebody else creates another, totally different, program which mimics the "look and feel" of your program perfectly. Have they violated your intellectual property? Some major computer companies would say yes and they have taken other companies to court over it. Other people would say no and point to the fact that no such restriction exists on copying the "look" or "user interface" of any other product type. What is your view on this? Do we need a new type of design right to protect the look and feel of things or would this just force every new product to be incompatible with everything else?

2.3.3 Data protection

Data protection legislation is becoming very widespread. The three pillars of such legislation are necessity, accuracy and privacy. Whilst these three concepts are often wrapped up in a larger number of data protection principles, the important protections which they enshrine are that personal data relating to individuals -

- Should only be held if necessary to the task in hand
- Must be maintained as accurately as possible
- Should not be disclosed to anybody else

This last requirement probably represents a historic first in that it imposes a legal imperative which can only be met with technological solutions. The non-disclosure aspect of data protection laws places a legal obligation on the holders of such information to implement a raft of security measures ranging from access control procedures to data encryption. In this day and age it would not be accepted that reasonable measures had been taken to prevent unauthorised disclosure if such security mechanisms were lacking.

2.3.4 Computer misuse

Computer misuse legislation comes in as many forms as there are forms of computer misuse. Unauthorised access and unauthorised modification of data are commonly made criminal offences under such legislation but they are rarely the crimes for which criminals are really investigated. Charges of unauthorised access and data modification are normally brought as part of a much larger case, such as fraud. These larger crimes are covered by conventional criminal law and the specific computer misuse elements tend to play a small part in the overall case. Penalties for computer misuse alone seem commonly to have been set to deter mischievous teenagers rather than career criminals.

There is an increasing number of voices arguing for legislation to criminalise computer based obscenity and defamation but there are global differences in cultural and political perspectives on what is acceptable in these areas so an international consensus is unlikely to be achieved for some time, if at all. This is not to say that you can ignore these issues though. Most jurisdictions have laws banning certain forms of material and you should make yourself aware of those that affect you.

2.3.5 Computer evidence

We end our examination of computers and the law with a word of warning about computer evidence. Crimes involving computer technology can often only be proved in a court of law by means of audit trails, access logs, etc. However, the justice system is all too well aware of the fact that evidence can be tampered with. What easier form of evidence is there to tamper with than a computer file? Files containing trails and logs are just as easy to edit as any other files. In order to preserve the chain of evidence contained in these files it is essential that they are not accessed or modified subsequent to a crime or they may not be usable as evidence. So if you think any computer for which you are responsible might have been used to perpetrate a crime think twice before looking at the log files with an editor - isolate the computer and call in the experts.

2.4 Ethical decision making

Computer ethics, or at least the publishing of books on the subject, became something of a boom industry in the last decade of the twentieth century. It is not hard to see why. The influence of computer technology on so many aspects of people's lives was advancing at an alarming rate. More alarming still, to the media anyway, was the apparent lack of morality of the young people destined to be the future of the profession. They were hacking into top secret facilities, creating computer viruses, spreading pornography. What they needed was a good dose of old fashioned ethics to set them straight. Hence all the new modules in computing degrees entitled "Computer Ethics" or something similar and thence all the books to support those modules.

We shall not insult you by trying to give you a moral code here. We trust that you have one already. What you might lack is the wherewithal to apply your moral values to the complex and confusing world which computer and communications technology have created and in which you now find yourself so thoroughly immersed. Perhaps you find even that suggestion somewhat patronising? If so, we apologise but one thing the author of this unit has identified is that computer professionals are not at their most articulate when discussing ethical issues and their ability to justify their actions often leaves a lot to be desired.

The twin aims of this section are to introduce you to some methods which can help you think through an ethical dilemma and to assist you in explaining your decisions in ways which indicate that you have, indeed, thought about their consequences for all concerned.

2.4.1 Moral systems

There are many moral systems. Best known amongst them are those espoused by the great world religions. If you are religious you should have no difficulty in writing down the fundamental moral tenets of your religion which guide the way you treat other individuals and the responsibilities you have towards the wider community. If you are not religious then your moral lights might not be so readily expressed in time-honoured phrases but now would be a good time to pin them down to words on paper. At this point most of the aforementioned ethics texts present a potted history of European moral philosophy from the ancient Greeks down to the nineteenth century. If you think Plato, Aristotle, Kant or

Mill might help you, feel free to make use of them. See Quinn (2005) amongst others.

The important thing to remember about the statements you have written down is that they apply to, and in, everything you do. They do not belong in a separate "non-technological" part of your life. They are the axioms which will help you wrestle with ethical problems and which will enable you to explain your decisions to others. All too often technologists feel obliged to explain themselves in a dispassionate and technical fashion which only fuels the concerns of those who would rather see some evidence of basic humanity. This does not mean that you should get all emotional and irrational. Rational thought and argument, weighing things in the balance, remain essential. You still need to be able to say things like -

In coming to this decision I gave due consideration to the consequences for X but concluded that they would be less severe than the impact on Y for the following reasons...

but by stating the moral cases for considering X and Y in the first place, even though they might seem obvious to you, you can re-assure people who might find the technology and the technical arguments intimidating.

2.4.2 Stakeholders

Kallman and Grillo (1993) suggested a very useful approach to making ethical decisions - whether this be to determine the morality of somebody else's actions or to help determine an ethical course of action to follow yourself. Their approach is to list all of the stakeholders in the decision.

Anybody who might be affected, either positively or negatively, by the choice being made should be given proper consideration. Stakeholders are not always easy to identify - some are only affected very indirectly. It can be helpful to tabulate the options and the stakeholders, noting the effect of each option upon each stakeholder.

2.4.3 Ethical tests

Kallman and Grillo also produced a collection of useful tests which we extend slightly for presentation here -

The Golden Rule

Treat others as you would have them treat you.

Other Person's Shoes Test

Does what you are proposing treat others as you would have them treat you if you were in their position rather than yours (cf. The Golden Rule).

Legality Test

Is what you are proposing legal?

Smell Test

Does what you are proposing smell right?

Parent Test

Would you tell your parents what you are proposing?

Media Test

Would you be happy for the media to find out what you are proposing?

Market Test

Is your proposed course of action such a good thing that you could actually sell it?

Always identify the important stakeholders and the key facts of a situation. It can help to write them down. Clarify the options open to you. Apply as many tests to each option as you feel are appropriate and consider the impact on the various stakeholders. Do this and you are unlikely to be accused of not giving due consideration to the consequences of your decisions.

2.5 Assigned task

You should select one of the following two ethical dilemmas and write a 2000 word essay discussing what you would do in that situation and why. This essay should be submitted at your second tutorial meeting.

1. Screen Capture Program

You are to imagine that you have recently become a development manager, overseeing a number of programmers and analysts working in project teams.

Three weeks ago, whilst browsing through a directory of materials which you have inherited from your predecessor, you discovered an application that lets you capture and view a snapshot of any of the screens used by the staff for whom you are responsible. Tactful enquiries on your part over the following weeks reveal a number of facts -

- Nobody knows about the existence of the screen capturing program
- About a year ago there had been a problem with productivity when certain staff had devoted a not inconsiderable amount of their working time to solving puzzles which they circulated amongst each other via e-mail
- Your predecessor had, apparently coincidentally, caught many of the offenders with these puzzles open on their screens and had reprimanded them
- Puzzling then dropped off and productivity picked up
- Productivity seems to have declined again since your predecessor left

You must now decide what to do about the screen capturing program. Discuss the ethical issues involved and come to a reasoned decision which you can justify to others.

2. Carcinogenic Fertiliser Data

You are to imagine that, at some point in the not too distant future, you have taken up a position as a systems analyst with a major agro-chemical company. After an initial period of fairly trivial work your employers entrust you with the processing of confidential data concerning a very promising new fertiliser for wheat. This you regard as a great accolade; since you are aware of the tremendous importance your company places on secrecy. Indeed, only some six or seven people in the whole enterprise have access to the data you have been charged with handling.

Three years later you have progressed well within the company and have been given much responsibility. You have been amply rewarded by your employers for the many evenings and weekends which you have devoted to your work. You have married and now have two children as well as a large mortgage and two nice cars bought with a loan from the bank - your assets are all invested in your house.

Then, the following year, disaster strikes; mortgage rates shoot up, house prices plummet, your partner (whose income has been on a par with yours) loses his/her job and, in the course of your work, you learn that the company has discovered that at least 70% of the people who have consumed the wheat grown with that promising fertiliser of four years ago have contracted cancer.

On questioning your supervisor of four years ago about the fertiliser you are informed that nobody outside the company is likely to discover the connection and you realise that the company is planning a cover-up. Anybody within the company who breathes a word about the scandal will be sought out and peremptorily dismissed.

You must now decide what to do about what you know. Discuss the ethical issues involved and come to a reasoned decision which you can justify to others.

2.6 Assignment

End of Topic Test

Q1: Which of the following is not a professional body -

a) Association for Computing Machinery
b) British Computer Society
c) Institute for Electrical and Electronics Engineers
d) International Standards Organisation

Q2: The computer-based ISO 9000 certification system is known as -

a) CrossOFF
b) LickIT
c) TickIT
d) TickOFF

Q3: The international security management standard is -

a) BS 5750
b) BS 7799
c) ISO 17799
d) ISO 9000

Q4: In law, a "tort" is a -

a) Duty
b) Right
c) Wig
d) Wrong

Q5: Screen displays with their accompanying button layouts, etc. are called -

a) Footprints
b) Look and feel
c) Look and learn
d) Stereotypes

Q6: Which of the following was NOT suggested as a pillar of data protection -

a) Accuracy
b) Longevity
c) Necessity
d) Privacy

Q7: The criminalisation of what is beginning to be talked about -

a) Computer games
b) Computer-based obscenity
c) Hacking
d) Unauthorised computer access

Q8: A chain of evidence can be broken by doing what to a log file -

a) Editing it
b) Opening it
c) Reading it
d) Selling it

Q9: Which of the following ancient Greek philosophers was mentioned -

a) Diogenes
b) Plato
c) Socrates
d) Zeno

Q10: Which of the following asserts that you should treat others as you would have them treat you -

a) Bronze Axiom
b) Golden Rule
c) Platinum Lemma
d) Silver Theorem

2.7 References

Quinn, M.J., 2005, *Ethics for the Information Age*. Addison Wesley.

Kallman, E.A. & Grillo, J.P., 1993, *Ethical Decision Making and Information Technology*. McGraw-Hill.

Seddon, J., 1997, *In Pursuit of Quality: The Case Against ISO 9000*. Oak Tree Press.

Topic 3

Risks and Threats

Contents

Learning Objectives

- *Familiarity with the concept of a computer crime*
- *Appreciation of the possible forms of computer misuse*
- *Familiarity with the security measures which can be used to prevent crime*
- *Awareness of the privacy issues relating to computer crime prevention*

3.1 Introduction

In this topic we shall examine the various forms of computer crime and the security mechanisms which can be used to deter or prevent them. We shall also discuss the privacy issues which arise from the use of some of the security techniques.

It is important to keep the effects of computer crime in perspective. The most common breaches of system integrity result, not from criminal acts, but from computer crashes due to power failures and untested software. Some of the most expensive breaches to rectify are those caused by non-computer related events such as floods and fires.

You should note that surveys which attempt to quantify breaches of system integrity and estimate their costs are notoriously inaccurate. Organisations, are very reluctant to publicise these breaches in case they lose the confidence of their customers or clients. Cases of fraud, in particular, are very rarely reported but a single incident of fraud can result in enormous losses.

3.2 Computer Crime

We shall investigate five classes of computer crime ranging from the rather mundane theft of computer equipment to the electro-magnetic emissions technology used for eavesdropping and from piracy to the e-mail viruses which plague modern-day computing.

3.2.1 Theft

Computer theft can take a number of forms. The most obvious is the physical stealing and taking away of computer equipment. Physically depriving the owner of their property in the conventional sense of the term theft.

Theft in the computer world, however, can also occur without necessarily depriving the owner of their property. Depriving somebody of an exclusivity right is theft. Taking a copy of something, for instance. This doesn't necessarily involve infringing their intellectual property rights. It might simply be a case of violating their privacy.

3.2.2 Piracy

Piracy is the term used to describe that form of theft which deprives somebody of an intellectual property right. Infringing a copyright, patent, design right, trademark, etc. Intellectual property rights exist to reward the originators of an idea or work or brand for making their intellectual property public so that the rest of us can benefit from it.

Piracy is effectively stealing the originator's revenue. The copying of computer programs or files and the unscrambling or decrypting of protection mechanisms are generally held to be acts of piracy.

3.2.3 Espionage

Espionage is the stealing secrets, the acquisition of confidential information. We shall briefly examine two ways in which this can be achieved - one software, one hardware.

- **Sniffers**

  Computer networks share communications channels so any node on a network can receive transmissions intended for other nodes. Normally a node would discard any packets not addressed to it but it is possible to configure nodes to be "promiscuous" and receive all packets. A sniffer program runs on a promiscuous node and inspects all of the packets on a network - particularly start of session packets which convey username and password details. Encryption can be used to prevent sniffers from making sense of the information sniffed but it incurs a network overhead, of course.

- **TEMPEST**

  Data can be captured from screens, keyboards, even disk accesses using TEMPEST - the Transient Electro- Magnetic Pulse Emission Standard. Obviously encryption can't be used to protect the data sent to display screens. However a variety of techniques can be used to scramble the data in such a way that a human can still make sense of what appears on the screen whilst the eavesdropper cannot.

3.2.4 Fraud

Fraud is to gain a financial or other personal advantage by deceit. The key word here is "deceit". It is impossible to estimate how much financial fraud occurs, with or without computer assistance. The only guarantee is that fraud will always be grossly under-reported by the victims. The scandal of large scale fraud can bring companies to their knees. Recall the case of Barings bank which was eventually sold for a song after a fraud scandal. A rule of thumb commonly used for estimating the true cost of fraud is to multiply the reported figures by ten.

One of the earliest forms of computer-based fraud was the "salami technique". Most banks refuse to deal with amounts smaller than a certain limit, typically the smallest coin in use. Certain calculations, such as interest payments for instance, can result in account balances which violate that rule. For instance, in the UK at the present time the smallest denomination is a penny. A calculation which results in a balance of 10.3 pennies will be turned into a balance of 10 pennies. Where did the 0.3 of a penny go? Well, into the bank's profit effectively because it certainly didn't get credited to the customer. The salami technique involved picking up all those extra small bits of money, which you could argue really didn't belong to anybody, and syphoning them off into another account where they could accrue into some very large sums indeed. Nowadays the salami technique refers to any process by which small amounts of money, sufficiently small to be unnoticed, are sliced off an account balance.

3.2.5 Sabotage

Sabotage can be thought of as reducing the effectiveness of a system through deliberate destruction or damage. Denial of service attacks, spam, viruses, worms, Trojan horses and bombs come into this category. We shall now clarify what all of these terms mean. Further details can be found in Grimes (2001).

- **Denial of service**

  Making multiple simultaneous accesses to a node on a network so that it becomes swamped with dealing with those accesses and can no longer do anything else, including serving further accesses. Web servers are a common target for such attacks but they are usually quite short-lived in duration.

- **Spam**

  Unsolicited, or unwanted, e-mail messages. In small quantities spam can be quite innocuous but few computer users remain untroubled by it these days. Spam filters, which score incoming e-mail messages against a number of well-known characteristics of spam, are the best defence at present since nobody seems prepared to take responsibility for tracking down the spammers and stopping their activities at source.

- **Virus**

  A virus is a self-replicating code segment which is embedded in larger host program. A virus will typically be activated when the host program is executed and copy itself into other programs. It will then modify the new host to make sure it gets executed when the new host is accessed or run. As anti-virus software becomes more adept at identifying and dealing with viruses so more advanced viruses seem to be released. The latest stealth viruses go to great lengths to hide their existence and polymorphic viruses camouflage themselves so that the tell-tale signatures which the anti-virus software uses to identify them change on every new replication. The best defence against viruses remains anti-virus software but it is crucial to keep the virus definition files used by such software up to date. Anti-virus software is only as good as the data it uses and new viruses are being released all of the time.

- **Worm**

  A worm is a self-replicating program which spreads across a network by copying itself to connected hosts. Unlike a virus, no carrier program is needed. In recent years the term worm has come to be used to describe viruses which spread across networks using e-mail attachments. Viruses carried by e-mail messages, purportedly sent by somebody the recipient knows, have wreaked havoc by using people's address books to e-mail themselves from one victim to the next. Most anti-virus software can identify these forms of virus - as long as the virus definition files are maintained properly.

- **Trojan horse**

  This is a program which apparently performs a useful function but which includes hidden destructive code. Known Trojan horse programs can also be identified by most anti-virus software.

- **Bomb**

  A bomb is a trigger which can activate malicious code, such as a virus. There are two common types - the logic bomb and the time bomb. A logic bomb monitors system activity and detonates when a particular event occurs or when an event has occurred a given number of times. A time bomb monitors the system clock and detonates at a particular time or on a particular date.

3.3 Security and Privacy

Security systems employ a variety of techniques ranging from the verification of identities, authentication of messages and encryption of data to the prescription of access controls, recording of audit trails and performance of risk analyses. We shall examine some of the methods used for verification and encryption in the following subsections. Further details can be found in Garfinkel and Spafford (2002).

Verification mechanisms are generally based on something possessed by the person whose identity is to be verified or something known only to them or some personal characteristic. Authentication systems can validate the originator of a message and confirm that its content hasn't been tampered with using certificates, digests or digital signatures. Finally, for confidential information which shouldn't be read by unauthorised people, the content can be hidden from prying eyes with encryption algorithms.

3.3.1 Something Possessed

Magnetic strip cards will probably be the most familiar example of this form of verification technique. The main problem with them is that they can be lost, stolen and forged. Mechanisms which have been employed to make the forger's task more difficult, but not impossible, can include

1. Watermarking the magnetic tape with an underlying non-erasable pattern and using an extra data track to check that it has not been tampered with.

2. Using a sandwich tape which has two layers of differing intensity such that any attempt to re-write the high intensity data would wipe out the low intensity background.

3. "Chip and pin" cards which have a much larger data storage capacity and can also perform some on-card processing. Typically the storage capacity will be 8K bytes as opposed to 250 bytes and the processing capability means that the card can be challenged to produce the correct response to many different verification requests.

3.3.2 Something Known

Passwords can pose security risks if they are not chosen wisely, changed regularly or used sensibly. You will probably be familiar with a kind of password called a non-unique password. This kind of password enables a person to confirm a claimed identity - typically the identity associated with a username. There are, however, a number of other types of password system.

Group passwords are shared by many people and are used when a number of different people all need access to the same thing. Unique passwords are used to claim an identity. They are a username and password combined. Variable passwords can be used in more critical installations to ensure that the password changes on every use. Each time the password is used a new one is derived from the previous one. Finally, where the ultimate in security is required, there are single-use passwords which are changed after each access, not using a rule as in variable passwords, but by using the next password from a previously drawn up list. The banking system employs single-use passwords and the password lists are couriered out to the banks at the start of each working day.

Password selection is the weakest link in the security system chain. If users are given a free choice of passwords the results can be highly susceptible to guessing or cracking. In general people do not choose sensible passwords and it only takes one poor choice to undermine a system. Furthermore passwords may not be changed very often. Again, it only takes one lazy person to undermine a system.

Automatic system allocation of passwords using password generators is not necessarily more secure than freely chosen passwords. Unmemorable passwords can be generated in this way and these are bound to be written down. Smarter generators try to produce pronounceable words as passwords, with varying degrees of success.

3.3.3 Personal Characteristics

If something possessed and something known are not practical or sufficient then we must turn to something "about" a person. Some personal characteristic which is unique to them. This is the field of biometrics.

There are two main types of biometric, physiological and behavioural. Physiological biometrics are physical characteristics which can usually be seen and measured in some way. Behavioural biometrics, on the other hand, are the result of some involuntary action such as a signature or a voice print.

We shall now look at the most common forms of both classes of biometric. We shall then briefly discuss some of the privacy concerns that have arisen as a result of the increasing likelihood of our being identified by biometrics in the future.

- **Physiological biometrics**
  - **DNA**

    Over 99% of our DNA is identical and so no use in identifying a given individual. DNA tests actually use the "junk DNA" which we all carry around but make no use of. DNA is not unique. Identical twins have identical DNA. Consider the following

    1 in 83 births in the USA is a twin

    28% of twins are identical and so have identical DNA

    Therefore 1 million people in the USA do not have unique DNA
  - **Face**

    There are two types of system used for face recognition. The first uses facial metrics. These measure specific features such as the distance between the inside corners of the eyes or the distance between the outside corners of the eyes and the mouth. These measures are then stored for comparison. The second method is based on "eigenfaces". An eigenface is a stereotypical face against which the face to be recognised is compared. Typically the degree of fit with forty carefully chosen eigenfaces might be recorded for each individual.
  - **Fingerprint**

    Not even identical twins have the same fingerprints. Computer-based fingerprint checking does not use the loops, whorls, etc. that we do. Automated Fingerprint Identification Systems (AFIS) record the locations of around ninety minutiae - places where a ridge starts or forks. If this is done for each finger and thumb then about nine hundred minutiae are stored per person.

- **Hand geometry**

  Geometric techniques produce small data sets and do not discriminate well. The geometry can be ascertained in two ways - using a mechanical device or using edge detection from an image. Hand geometry uses estimates of finger lengths and thumb widths to identify an individual. A reduced form of the hand geometry approach uses the geometry of just two fingers.

- **Iris**

  Iris scanning seems to be the most robust and most accurate biometric discovered to date. Standard video cameras are sufficient to capture the images. The probability of two irises having the same biometric value is 1 in 10^{78}. Even identical twins have different iris patterns. A typical iris recognition system stores just 256 bytes per person.

- **Retina**

  Blood vessel patterns in the retina are unique. To identify somebody from their retina they must look through an aperture and align their eye with the aid of target circles projected to help them. Infra-red light illuminates the retina to enhance the image of the blood vessels and a camera captures the image. Comparison can then be performed against previously captured images.

- **Vascular**

  As with retinal scanning, infra-red light is used to illuminate the blood vessels under the skin and a camera is used to capture an image. This technique can be used on readily accessible parts of the body such as the face, back of the hand or wrist.

- **Behavioural biometrics**

  - **Signature**

    The best systems do not treat this as a pattern recognition task because signature repeatability is generally quite poor. The dynamics of the pen motions are the key properties used - accelerations, directions, pressures and stroke lengths. Capturing these features is not easy and consistency is difficult to achieve.

  - **Voice**

    Voice recognition is a pattern recognition task. A set phrase is used to create a voice print template. The phrase needs to be repeated several times during the creation of the template. Subsequent entry of the phrase can then be compared against a number of templates and the identity of the speaker retrieved. This technique attempts to be invariant to the physical characteristics of a voice but can become dangerously dependent on the behavioural characteristics of speech so somebody with a cold might not be recognised.

- **Privacy concerns**

  Biometrics, because they are so personal, have highlighted concerns about personal privacy and freedoms. Whilst nobody would object to being identified on those occasions when they choose to be, such as when accessing their bank account, surveillance techniques could take advantage of biometrics to identify us without us knowing about it. Some people find this very worrying (Garfinkel 2000). Developers and users of this technology need to be aware of and understand these concerns.

3.3.4 Cryptography

Cryptography is the art of hiding the content of a document or message from unauthorised people. The aim is to ensure that only those people who you wish to read the text can actually do so. Modern encryption techniques are not uncrackable, they just require an impractical amount of time to crack - many years, even with the fastest computers.

The algorithms used in modern cryptography are not secret. They are published for all to see and use. They rely for their power on keys which are large numbers known only to the sender and receiver of the message. In private key cryptography, such as the Data Encryption Standard (DES), the decryption algorithm is simply the inverse of the encryption algorithm and one key is used by both the sender and the receiver. This key must be kept secret. To crack the code one has to find the key.

One of the most effective and popular encryption algorithms is the Rivest, Shamir and Adleman, or RSA, algorithm (Garfinkel and Spafford 2002). This algorithm is actually two slightly different algorithms, one of which encrypts and the other of which decrypts. Two keys are required because each algorithm uses a different key. As long as the keys have been chosen carefully then knowledge of the algorithm and one of the keys will still leave the cracker requiring an enormous time to discover the other key.

Public key cryptography makes use of the fact that one key (the public key) can be released to everybody so that they can encrypt messages but not decrypt them. To decrypt a message a private key is needed and this is kept secret by the recipient of the messages. In this way anybody can send a secret message, such as the password for their bank account, but only the receiver, the bank, knows the other, private, key so only they can decrypt it and authorise access to the account.

3.4 Assessment

Assigned Task

You should write a 2000 word essay on one of the following two topics. This essay should be submitted at your third tutorial meeting.

1. **Detailed Working of Biometrics**

   Research and describe the detailed working of one example from each of the two main categories of biometric; physiological and behavioural.

2. **Reliability of Biometrics**

   Physiological biometrics identify bodies or, more specifically, parts of bodies. They do not identify people directly. Furthermore, all biometric data must be stored for subsequent comparison and it is a match between the presented and the stored data, which might not be the correct data, that is used for identification. Discuss the problems which these two levels of indirection might create.

End of Topic Test

Q1: Which of the following was NOT suggested as a form of computer crime?

a) Debugging
b) Espionage
c) Fraud
d) Sabotage

Q2: Sniffer programs make use of what type of network node?

a) Client
b) Naked
c) Promiscuous
d) Server

Q3: Fraud is to gain personal advantage by

a) Deceit
b) Hacking
c) Surveillance
d) Theft

Q4: Slicing small amounts of money off bank accounts is called the

a) Bratwursting
b) Hot dogging
c) Salami technique
d) Sausage method

Q5: Which of the following were NOT cited as a form of sabotage?

a) Bombs
b) Explosives
c) Viruses
d) Worms

Q6: Authentication systems may employ

a) Access controls
b) Digital signatures
c) Hall marks
d) Lie detectors

Q7: Which of the following was NOT suggested as a verification technique?

a) Letter of recommendation
b) Personal characteristic
c) Something known
d) Something possessed

Q8: A behavioural biometric results from what kind of action?

a) Aggressive
b) Involuntary
c) Physical
d) Voluntary

Q9: Which of the following was NOT cited as a type of biometric?

a) DNA
b) Fingerprint
c) Hair colour
d) Signature

Q10: How many keys must be kept secret in public key cryptography?

a) All
b) None
c) One
d) Two

3.5 References

Garfinkel, S., 2000, *Database Nation.* O'Reilly.

Garfinkel, S., and Spafford, G., 2002, *Web Security, Privacy & Commerce.* 2nd edition, O'Reilly.

Grimes, R.A., 2001, *Malicious Mobile Code.* O'Reilly.

Quinn, M.J., 2005, *Ethics for the Information Age.* Addison Wesley.

Topic 4

Dependence and Change

Contents

Learning Objectives

- *Deliberation on the relationship between technology and society*
- *Awareness of the impact of technology on society*
- *Awareness of the influence of society on the development of technology*
- *Understanding of the degree of dependence of modern society on technology*

4.1 Introduction

We have already mentioned the degree to which modern society has become dependent on technology. The impact of technologies such as the motor car, the telephone, television, etc. are well documented. The impacts of computer technology are still being discovered but much has already been written about them. We shall attempt to summarise the current situation in this topic and look to the future in the next topic.

It is important to note, however, that there are two cause and effect relationships at work. It is not only the case that society is influenced by technology. The direction and speed of technological development is also heavily influenced by society. Since this latter relationship is often hidden and working behind the scenes we shall devote more space to it here than to the more obvious influences in the other direction.

Computer technology, like any other technology, brings risks as well as benefits. Indeed, the ubiquity of computer systems means that there are probably more such risks, with greater potential dangers, inherent in computer technology than any other that mankind has had to deal with (Neumann, 1995). We shall consider a particular class of computer system known as a safety-critical system in which failure would be disastrous and we shall look at some systems where that disaster actually occurred.

The best known example of our dependence on computer technology was the Year 2000, or Y2K problem, also known as the Millennium Bug. We shall examine this as a case study in computer dependence but also as a study in the trust which the world now has to place in the computer industry and computer professionals. Are we living up to that trust? Many would say the Y2K problem showed that we are not.

4.2 Technology and Society

Technological developments affect society at large both directly and indirectly. There are few aspects of our work, recreation, domestic life, welfare or law enforcement services that are not affected by computers (Baase 2003, Spinello and Tavani 2001). Try thinking of some daily activity that has not been affected by computer technology. It won't be easy. Brushing your teeth, perhaps? Your toothbrush and your toothpaste were both almost certainly developed with computer assistance. The water arriving at your tap has probably been delivered with the assistance of computer control at some point in its journey. I could go on but I'm sure you get my drift and I do not wish to dwell on the broader impacts of technology on society with which I am sure you are already very well acquainted.

It is the influences in the other direction which are not so obvious. Societal factors can, and do, affect the speed and direction of technological developments (Bijker et al., 1989). They always have but it is indicative of how little recognition we give them, that we have great difficulty in recollecting any examples. Try thinking of some. Again, it won't be easy. Commercial, political, cultural and economic pressures and choices have had a considerable impact on the technology we see around us. It is worth looking at a couple of examples from the past even though, by definition, they will mostly pre-date computer technology (MacKenzie and Wajcman, 1985).

4.2.1 The Refrigerator

At the turn of the twentieth century, the idea of a refrigeration machine was conceived. The key question at the time was how to power it. Gas or electricity? You know the outcome but do you know why? Let's look at the issues.

Gas refrigerators have hardly any mechanical parts whilst electric refrigerators need a compressor and a motor. Therefore gas machines are much less likely to break down. The early electric models made a lot of noise and even nowadays they aren't silent, as gas ones are.

Gas supplies were more prevalent than electricity supplies. Gas had been around longer and the infrastructure was therefore more extensive. More homes could take advantage of a refrigerator if it was powered by gas.

The gas refrigerator was supported by two comparatively small companies - Servel and SORCO - whilst the electric refrigerator was supported by three giants - General Electric, General Motors and Westinghouse.

The power behind modern day refrigerators is electricity and not gas because of commercial power, not because it was the best decision technologically.

4.2.2 The Machine Tool

By the middle of the twentieth century it had become possible to develop an automatic version of the machine tools used by skilled craftsmen for high precision metal working. These machines would do the job of the machinists more consistently and for longer periods at a time. The issue here was how they were to be instructed what to do - by recording, and then playing back as often as you liked, the actions of a skilled metal worker or by using a numerically controlled (NC) machine which had to be programmed.

The record/playback approach was comparatively cheap, whilst the NC machines were very expensive.

The record/playback machines used a skilled metal worker which would seem to have been an advantage over the programmers, with little metal working knowledge, necessary for the NC machines.

However, these machines became the subject of hot political debate in certain quarters, notably the United States Air Force (USAF). Machine tools were used for the high precision metal working necessary in aircraft production. There were, almost certainly unwarranted, concerns at the time about the reliability of workers who belonged to trades unions and the option of eliminating the need for these workers appealed to a number of politicians.

The outcome was that the supporters of the record/playback approach were bought out. Not only that but, because the NC machines were so expensive that the suppliers who were to use them couldn't actually afford them, the USAF paid for the installation of the machines in the sub-contractors' factories.

It is an ill wind that blows nobody any good, and it must be said that although the decision to develop NC machines was a political one, with little technological or economic merit, NC became an important driving force in the early development of computer aided manufacturing.

4.2.3 The Computer Industry

You may be thinking that the refrigerator and the machine tool are a long way from the modern computer industry and we have little to learn from such examples. There are, however, plenty of examples to be found in the world of computer technology. The trouble is that the technologies that weren't taken up and developed aren't here now, by definition, and so we can't see what we are missing or what might have been.

One of the early battles in the modern era of computing, and there were plenty of others before the modern era, was fought between Intel and Motorola. Both companies set out to produce 16-bit processor chips. Motorola's 68000 chip was a full 16-bit chip with both address and data buses being 16-bit. Intel's 8086 chip, however, whilst it had a 16-bit address bus, had only an 8-bit data bus. In the transition from 8-bit to 16-bit, Intel had only gone half-way, two fetches were needed by the Intel chip to retrieve the full 16-bits of data and it was thus slower than Motorola's offering. When IBM launched their personal computer, which spawned the home computer revolution, they chose to use the Intel chip rather than the superior Motorola one. Motorola continued to make superior chips, generally keeping one step ahead of Intel but selling to a much smaller market than Intel had cornered thanks to IBM and the IBM compatible PCs, most of which have an Intel inside to this day.

The Apple Macintosh, which was in many respects superior to the IBM PC, used Motorola chips but such was IBM's dominance of the market that Apple computers remain the computer of choice for only a small proportion of the world's computer users.

Another company to benefit from IBM's early dominance was Microsoft. You won't need to be told how dominant Microsoft has become but you might pause to ponder on where we would be today if Apple and Motorola had enjoyed the same success as IBM and Intel. Would Microsoft have backed both horses perhaps, or might they have chosen the wrong one and remained a small player in the computer world?

In recent years Microsoft have had to fight a number of legal battles to defend their proprietary software from the ever-increasing volume of open source software which is threatening some of their key products - their MS Office suite of programs, their MIE web browser and even their MS Windows operating systems. Are Microsoft just too big a company to lose out in the long term? We shall have to wait and see but, whether we approve of Microsoft's current dominance or not, we should never gainsay the enormous contribution it has allowed them to make to all of our lives.

4.3 Safety-Critical Systems

Our dependence on computer technology is at its most sensitive when we put our lives in its hands. Hazard analysis and risk assessment are essential steps in the development of a system where safety is critical (Levenson 1995).

4.3.1 Hazard Analysis

Hazard analysis is the first step in ensuring that a system will cope with all the eventualities that it might encounter. The analysis starts with hazard identification; determining the hazards that might exist when the system is used. These hazards should then be classified according to their severity and likelihood of occurrence. Each hazard should then be decomposed in order to identify the precise circumstances under which it will arise.

4.3.2 Hazard Severity and Likelihood Categories

The US Department of Defense uses four categories to identify the severity of a hazard. They are, in descending order of severity, Catastrophic, Critical, Marginal and Negligible. Levenson (1995) recommends six categories of hazard likelihood. In descending order of likelihood they are Frequent, Probable, Occasional, Remote, Improbable and Physically Impossible.

4.3.3 Risk Assessment

The final risk assessment has to balance a number of things. Costs and delivery times are the main factors which affect how much development time and effort can be devoted to safety measures. There is no such thing as absolute safety but worst case scenarios should be used to combine the hazard severity with its likelihood to ascertain whether the final system can be made safe enough and whether this can be accomplished within budget. It is quite proper for the risk assessment to conclude that the development should not take place if the hazards cannot be brought down to an acceptable level. What is acceptable, of course, requires professional judgement.

4.3.4 Failure Examples

We shall now briefly describe two notorious software failures. We leave you to judge whether negligence was involved.

- **Ariane 5**

  The explosion of the European Space Agency's Ariane 5 rocket on its maiden flight in June 1996 was caused by loss of guidance and attitude information shortly after lift-off. The official inquiry into the disaster found that this was due to specification and design errors in the software of the inertial reference system. The inquiry discovered that tests conducted on the system were inadequate. If they had been performed more thoroughly the disaster would probably have been avoided. Mercifully this was an unmanned mission and nobody was killed or injured. This incident demonstrates that computer software has become so complex that bugs can remain undetected, even in the incredibly thorough and safety-conscious world of space technology.

- **Therac-25**

  Between June 1985 and January 1987 there were six accidents involving massive overdoses of radiation from a Therac-25 radiation therapy machine. These accidents, which resulted in deaths and serious injuries to patients, were caused by software errors. The errors had also been present in an earlier model, the Therac-20, but because that was an older machine, there had been additional hardware safety mechanisms which had prevented the accidents. The more modern Therac-25, it had been felt, could rely on software safety mechanisms alone.

Y2K - A case study

The first thing to note about the Y2K problem was that it was more than one distinct problem. In addition to the issues surrounding the use of a two digit format for the year (the practice of dropping the 19 from the front of the year), there was a further problem in that the year 2000 was a leap year but not everybody knew it. The year 1900, for instance, hadn't been a leap year and the part of the leap year rule which applied to the year 2000 hadn't been applicable since the year 1600. So, in addition to the two digit year problem, there was also the possibility of some computer systems working on a 365 day year rather than a 366 day year and incorrectly leaving out the 29th of February.

However, we shall leave the leap year issue aside and concentrate on the problems caused by the two digit year format. The first problem is that if only two digits are used then time periods in excess of 99 years are not storable and might lead to systems crashing as a result of overflow problems. The second problem is that if you are dealing with dates that span the millennium boundary then the century becomes ambiguous and dates can be sorted incorrectly. The year 2000 should come after the year 1999 but if the first two digits are dropped from both then the year 00 will be sorted to fall before the year 99. The third problem, which made everybody hold their breath at midnight on the 31st of December 1999, was what would happen when the year 99 had 1 added to it? Would it try to become 100 and crash the computer? Would it become -1 with equally devastating results?

With so many computers out there, in people's homes, embedded in their domestic appliances, in safety-critical systems such as aircraft control systems, life support systems and nuclear power stations it is not surprising that many people, both within the computer industry and without, feared the worst. No system could be considered immune. System clocks and date reckoning could turn up in the least likely of places for no other reason than that they were a built-in function of the processor being used.

This was certainly a no-win situation for the computer industry. Firstly, and with some justification, they were blamed for the problem arising in the first place. In their defence though, we should point out that the industry had been aware of the problem for some time and had been warning organisations that their legacy (old) systems needed to be replaced or upgraded. The programmers of the 1960s and 1970s really hadn't expected their programs to still be in use at the turn of the century.

However, no matter where the blame lay, it was clear that if the computer industry encouraged governments and private industry to spend enormous sums fixing the problem then there wouldn't be problem any more and they would be accused of scare-mongering to increase their own profits. On the other hand, if they played the problem down then there would undoubtedly be catastrophic failures of some systems and they would be blamed for that instead.

There is no question that the Y2K problem was real enough. During simulations of the roll-over from 1999 to 2000

- All the computer screens went blank at the International Federation of Airline Controllers
- 4 million gallons of raw sewage were dumped onto a Los Angeles street

- A robot assembly line crashed at a General Motors factory and the security system prevented staff from leaving

Following the millennium there were

- Nuclear power plant failures in Japan, Spain and the USA
- Healthcare system failures in Brazil, Norway, Sweden and the UK
- Power distribution failures in Honduras and South Korea

All of these incidents were genuinely attributable to the Y2K problem. In the run up to the year 2000 though, it wasn't at all clear just how many such cases there might be.

World-wide, the cost of the Y2K fixes that were actually implemented has been estimated at £300,000 million. The USA alone spent £60,000 million, including £30 million on a special Y2K command centre. £20,000 million was spent in the UK but in Italy only £500 million was spent, including £1.5 million on billboards to warn people of the risk. Italy fared no worse than the USA or the UK as it turned out.

Perhaps it was what was learned from the Y2K problem that will, in the end, justify all the fuss it caused. Computer professionals learned that there was a lot of legacy software out there and the life expectancy of software was considerably longer than they had realised. They learned that most IT departments didn't have a clear idea what software they actually had and were using. There was a need for proper software inventory management, methodologies and tools. Computer users learned how reliant they had become on IT and that that reliance was both broader and deeper than they had realised. Company executives learned that IT had become too important to be left solely to the boffins. Managers, from the boardroom down, learned that they need to be considerably more critical of, and better informed about, IT solutions and practices.

What should the final verdict on the computer industry be? Take your pick

1. The fact that the Y2K problem arose demonstrates that the computer profession is immature and its practices are unsound
2. The computer profession's reaction to the Y2K problem was a triple success story

   i Success in raising awareness of the problem

   ii Success in persuading enterprises to invest in fixing it

   iii Success in fixing the problem
3. The computer profession refused to accept any liability for the problem, provoked widespread hysteria and then exploited the fear it had generated for financial gain

Here's a final thought. The Unix operating system uses a 32-bit signed integer to hold the time and date. This variable has been counting the seconds since midnight GMT on the 1st of January 1970. It will roll over to a negative number at precisely 03:14:07 GMT on the 19th of January 2038. Is that too far off to worry about?

4.4 Assessment

Assigned Task

You should prepare a 15 minute presentation on one of the following two topics. The presentation will be made at either your fourth or fifth tutorial meeting. Your presentation might benefit from a consideration of some of the issues covered in the next topic.

1. **Computer Games**

   Eugene Provenzo has compared computer games unfavourably with more traditional toys as follows

   "In the case of [computer games] the child has almost no potential to reshape the game and its instrumental logic. There is literally one path down which the player can proceed. The machine and its program impose an instrumental logic on the play situation and the activities of the child. In the light of evidence ... concerning the violence, aggression, and stereotyping found in these games, this fact is particularly disturbing."

   Eugene Provenzo, "Video Kids" Harvard University Press, 1991

   Computer games have advanced considerably since this was written but should we be any less concerned than Provenzo? Are there reasons to be even more concerned now?

2. **Open Source**

   The protagonists in the open source versus proprietary software debate have made the following statements

   "Digital information technology contributes to the world by making it easier to copy and modify information. Computers promise to make this easier for all of us. Not everyone wants it to be easier. The system of copyright gives software programs "owners", most of whom aim to withhold software's potential benefit from the rest of the public. They would like to be the only ones who can copy and modify the software that we use ... What does society need? It needs information that is truly available to its citizens - for example, programs that people can read, fix, adapt, and improve, not just operate. But what software owners typically deliver is a black box that we can't study or change."

   Richard Stallman, Founder of the Free Software Foundation
   "Why Software Should Not Have Owners", 1994

   "It [the GNU General Public Licence] also fundamentally undermines the independent commercial software sector because it effectively makes it impossible to distribute software on a basis where recipients pay for the product rather than just the cost of distribution ... Two decades of experience have shown that an economic model that protects intellectual property and a business model that recoups research and development costs can create impressive economic benefits and distribute them very broadly."

   Craig Mundie, Senior Vice President, Microsoft Corporation
   "The Commercial Software Model", May 2001

   To what extent do you agree with each of them? Are there elements of truth in both statements?

End of Topic Test

Q1: The Y2K problem was also known as the

a) Bug of the century
b) Millennium bug
c) Roll-over bug
d) Two thousand year itch

Q2: Societal factors can affect both the speed and what of technological developments?

a) Cost
b) Direction
c) Popularity
d) Size

Q3: Which of the following was NOT cited as a societal pressure on technological developments?

a) Commercial
b) Cultural
c) Fashion
d) Political

Q4: Which of the following pairs was NOT suggested as an advantage of gas refrigerators over electric refrigerators?

a) Availability of gas
b) Cooler
c) No mechanical parts
d) Quieter

Q5: Microsoft's and Intel's success was attributed to which company's market dominance?

a) Fujitsu
b) IBM
c) Motorola
d) Siemens

Q6: Which of the following is NOT one of the US Department of Defense hazard categories?

a) Catastrophic
b) Critical
c) Moderate
d) Negligible

Q7: The Ariane 5 explosion occurred in which year?

a) 1957
b) 1966
c) 1996
d) 2001

Q8: The Therac-25 accidents were attributed to what kind of error?

a) Hardware
b) Medical
c) Software
d) User

Q9: Which of the following is NOT a leap year?

a) 1600
b) 1900
c) 2000
d) 2004

Q10: What was the estimated cost world-wide of the Y2K problem?

a) £3 million
b) £30 million
c) £300 million
d) £300,000 million

4.5 References

Baase, S., 2003, *A Gift of Fire: Social, Legal and Ethical issues for Computers and the Internet.* Prentice Hall.

Bijker, W.E., Hughes, T.P. and Pinch, T., 1989, *The Social Construction of Technological Systems.* MIT Press.

Levenson, N.G, 1995, *Safeware: System Safety and Computers.* Addison Wesley.

MacKenzie, D. and Wajcman, J., 1985, *The Social Shaping of Technology.* Open University Press.

Neumann, P.G., 1995, *Computer Related Risks.* Addison Wesley.

Quinn, M.J., 2005, *Ethics for the Information Age.* Addison Wesley.

Spinello, R.A. and Tavani, H.T., 2001, *Readings in CyberEthics.* Jones and Bartlett.

Topic 5

Brave New Worlds

Contents

Learning Objectives

- *Understanding of the concepts and principles of open source*
- *Appreciation of future trends in IT and their potential impact*

5.1 Introduction

We shall round off this unit by considering some recent developments which are likely to have a significant impact on the way we develop and use information technology in the future. With the movement towards a greater acceptance of open source software (DiBona et al. 1999) we are seeing a return to the ethos that prevailed in the early days of computing when people willingly shared their files and programs. Software is becoming more freely available but not simply on our own computers. Pervasive systems running across wireless networks are making it possible for us to tap into services provided by others from almost anywhere (Saha and Mukherjee 2003). We can expect more and more of the services we use to be provided by these networks as time goes on. There is much to think about regarding the effect this might have on the way we live. Not least what might happen to those who are excluded or alienated from all of this technology.

5.2 Co-operative Computing

Co-operation was once quite normal in the world of computing. Prior to the 1980s source code was always made available - even for proprietary systems. Copyright and Patent Law should have protected intellectual property rights and fostered the dissemination of information. However, trust broke down and binary-only releases have now become the norm for proprietary systems. The sharing ethic of the pre-1980s has endured in a few places and seems to be taking off again. Trust, however, is essential for any form of co-operation.

The Free Software Foundation (Williams 2002) and the Open Source Initiative (Raymond 1999) have provided a way forward with tools such as Copyleft, the GNU General Public Licence and the Open Source Definition which provide protection to the originators of work that is released as open source. The success of Linux is a testament to the effectiveness of these protections and the quality of the software so developed.

Peer-to-peer networks (Oram 2001), the antithesis of the client/server approach to networking, have enabled like-minded individuals to come together and share files, sometimes controversially, without the need for a central repository. Co-operation and trust appear to be making a come-back.

5.2.1 Open Source

The increased interest and participation in open source developments have, as we have seen, led the purveyors of proprietary software to become very concerned. The Linux operating system is open source and can be downloaded from the Internet at no cost. New applications which run under Linux are being made available daily via web sites such as sourceforge (Sourceforge 2005) and even Microsoft is having to look to its laurels as the Linux snowball continues to gather momentum. Open source software has, of course, been written for other operating systems as well, including Microsoft's Windows family.

- **Copyleft**

  The trouble with making software freely available is that somebody else can pick it up, modify it slightly and then "take it private", or claim it as theirs. In order to protect free software from such a fate something akin to a copyright notice is required. Not the usual copyright notice that preserves all rights to the originator but a notice that gives away all rights except for the few necessary to prevent anybody else claiming all of those rights back again. This is the intention behind copyleft.

Copyleft gives permission to

- Run
- Copy
- Modify
- Distribute modified versions of a program.

Source code must clearly be made available for this, so binary-only releases cannot be covered by copyleft. Copyleft does not allow the adding of extra restrictions or taking the program, or modifications to it, private. Consequently the combination of copyleft code with non-copylefted code is non-trivial and this hampered the spread of open source software in the early days.

- **GNU**

  GNU stands for GNU's Not Unix and, whilst it was initially solely concerned with producing a free rival to the Unix operating system, it has become the "brand name" for many open source products. The GNU General Public Licence (GPL), in keeping with the notion of copyleft, forbids mixing GNU software with non-free software. The problems which this continued to create led to the GNU Lesser GPL (LGPL), which relaxed the non-mixing requirement for software libraries. That is, proprietary products could use open source software libraries under an LGPL licence.

- **Open Source Initiative**

  The Open Source Initiative was formed in order to take an even bigger step in permitting the mixing of open source with proprietary software. Open source licences confer a right to use modifications of the original open source in non-open applications. The Open Source Definition explicitly states that selling-on as part of an aggregate must be permitted under an OSD licence. Clearly, this permission to allow people to make money from the open source work of others is controversial but it was certainly key to the expansion we have witnessed in the use made of open source software.

5.2.2 Peer-to-Peer

Peer-to-peer systems aim to harness of the massive computational power and storage resources that even a few tens of computers can collectively deliver. They aim to support direct person-to-person (P-P) or application-to-application (A-A) network connectivity. Typically the nodes in the system would be home PCs dialling up via a modem. This meant that no one node could be relied upon to always be present. Thus, Peer-to-peer systems had to be decentralised and every node had to have a degree of autonomy. It is this decentralisation that has caused much of the controversy surrounding peer-to-peer systems. There is no ring-leader to take to court when these systems are used for exchanging files of pirated music for instance.

Apart from the technological aspects of the networks, peer-to-peer's biggest contribution has been in letting ordinary people publish to the world from their home PCs. Note that we are not simply talking about authoring. Anybody can author something on their PC but in order to distribute it to the wider community they would normally need access to a web server. Peer-to-peer systems remove that need; people can publish material directly from their own PCs. This ability has been dubbed the "Cornucopia of the Commons" because of the enormous variety of material which it permits to be broadcast. Sadly though, it has also sometimes been the "Tragedy of the Commons" with people freeloading off the publishings of others whilst offering nothing in return. Once again we find trust and accountability becoming critical elements of the system.

5.3 *e*Life

*e*Life is a term, coined elsewhere by this author, to describe what our lives might be like as the many and diverse "*e*" technologies of today and tomorrow make their unpredictable impacts upon us. Before exploring this technological dream world, though, we should pause and ask ourselves if it will be open to all. Exclusion and alienation of sectors of the community are a distinct possibility.

Exclusion is most likely to arise as a result of the cost of the technology, which may be beyond some people's means. Are there parts of the world which will be left behind as we race forward? Are their sectors within our own communities that will simply not be able to keep up with the cost of endless upgrades and so not be able to take advantage of all of the services on offer? People with disabilities might also be excluded from certain services if not enough thought is put into their delivery by service providers. Streaming audio and video should mean that very few services would be impossible to deliver in a suitable form to a deaf person or a blind person, etc. The cost of providing such services may mean that they are not though.

Alienation can come from being unfamiliar with the technology and so being afraid to use it. Fears that the older generation might fall foul of this seem, on the whole, to have been misplaced. Are there other groups within society who might be alienated though? Will some groups with special needs be alienated as a result of the exclusions we mentioned previously? Might they give up on the whole business if it requires an inordinate amount of effort on their part to access the services they want? Can we cater for people who are not disabled in the conventional sense, but become so because of our reliance on computer technology? People with numeracy and literacy problems for instance.

As information technology professionals we can't make poor people richer but we can, and should, be able to ensure that potentially high-risk groups are not disenfranchised by tomorrow's computer technology.

5.3.1 Technology

Finally, we can now ask what tomorrow's computer technology is likely to be like?

We already have embedded systems in car engine management systems, mobile phones, microwave ovens, washing machines, DVD players, etc. In the future we can expect software to be embedded in practically any piece of hardware that could benefit from adaptive control. The choice between a hardware or software solution which we are used to is likely to become a non-issue.

The Semiconductor Industry Association (SIA) predicts that it will soon be possible to place 100 million transistors onto a chip. It will be possible to put complete computer systems onto a single chip. This will take integration beyond VLSI and into System Level Integration (SLI) or System-on-a-Chip (SoC) technology. The design and verification of such systems will pose major challenges.

Micro Electro Mechanical Systems (MEMS) are currently in their infancy but they offer the potential for incredible miniaturisation of sensors, communications and actuators. Mechatronics in miniature, nanotechnology, molecular machinery and micro-motors are all examples of MEMs technology. There is tremendous scope for applications in medicine and healthcare. Pacemakers, cochlear implants, prosthetics, even nanorobots running around in your blood stream breaking up clots so you don't get thromboses. All sorts of mundane objects could become active and reactive.

Wireless networks come in two main forms nowadays; mobile phone networks and wireless LANs (WiFi). The latest mobile phones already use GPRS (General Packet Radio Services) which means they can be permanently online on a pay-per-byte basis. Wireless LANs permit computers to connect to Access Points on wired networks. Our mobile phones and many other devices could become nodes on Wireless LAN networks and thence connect to the Internet. Concerns over the security of wireless networks are being addressed by Extended Service Set ID (ESSID) and Wired Equivalent Privacy (WEP).

The Semantic Web is a vision of the World Wide Web in a machine usable form. Currently information is provided in a form suited to viewing by us. What if all the information could also be provided in a form suited to computer programs? We could send software agents out into the Internet to find appropriate information, combine it, perform calculations on it for us. A semantics is needed to describe each item of information so the agents could identify what was what (cf. Meta-tags).

We've already discussed Peer-to-Peer systems. We can expect these to spread but they have already made a contribution to the development of even more powerful systems such as Grid computing. The Grid is a reliable, scalable, heterogeneous, dynamic, global infrastructure which links a wide range of computing and non-computing devices. It offers enormous capacity in processing power and storage volume. It can also be used to make complete facilities available. Already Grid computing is being used to link scientific laboratories so that researchers in one lab can conduct experiments in other labs anywhere on the Grid.

Computing resources everywhere is a concept we have already mentioned in passing. There are two senses in which this can be viewed and both are currently under development. Pervasive computing conceives of computers everywhere in a "right here and now" sense. The Holy Grail is universal availability. Computers in everything - personal digital assistants (PDAs), mobile phones, wearable computers (in our clothes), smart buildings (Internet Zero). IBM has a whole division working on this paradigm. Taking a slightly different perspective is Ubiquitous computing which focuses on keeping the technology in the background; transparent and invisible. The Holy Grail here is for users to become oblivious to the technology which surrounds them. The late Mark Weiser, father of the computers everywhere concept, described this "calm technology" as follows

> "The ubiquitous computer leaves you feeling as though you did it yourself"

Computing resources might end up being supplied just like any other utility such as electricity, gas, water, etc. This idea has, not surprisingly, been dubbed Utility computing. Will it herald the return of computer bureaux? It might offer low entry cost options to enormously powerful information processing systems on a "pay as you go" basis. Service level guarantees will be required for such an idea to take off but if it does it will be the ultimate in outsourcing.

5.3.2 Society

How might the societies in which we live be affected by computer technology? This is difficult enough to predict without even considering some of the developments we have just presented.

Home-working is one thing we may see more of as improved technology makes it possible for us to be at work in a virtual sense whilst remaining at home. Before rashly assuming that improvements in the quality, cost and availability of streaming video systems and the like will make home working more attractive, we should ask if there might be other reasons why it hasn't already taken off. Productivity can be an issue for some home workers, distractions at home may lead them, or their bosses, to prefer the office environment. Maybe the personal contact we get at work is a key factor?

Perhaps developments in Computer Supported Co-operative Work (CSCW) could help? We're all doing CSCW already but in a hap-hazard and slip-shod fashion. We use mailing lists, discussion fora, etc. We pass documents and spreadsheets around amongst collaborators. CSCW sits between organisational and individual computing. Research into CSCW focuses on systems to support small groups of workers. CSCW is "socio-technical". Social scientists are needed to find out how we use, and what we want from, CSCW systems to make them more useful.

Where is *e*Commerce heading? There has been a remarkable take-up rate in online shopping. Data-mining techniques are likely to lead to better targeting of direct marketing which will be more acceptable to consumers. We might all end up using *e*Cash.

Could *e*Healthcare provide virtual surgeries on the web? Routine medical problems can probably be dealt with automatically, thus saving doctors' time for more serious cases. Perhaps video-streaming will enable doctors and patients to interact without the necessity of patients leaving their sick-beds?

Perhaps we will see the evolution of *e*Democracy. Virtual surgeries might facilitate communication between constituents and their representatives. Intelligent FAQs might be able to automatically answer common questions which constituents ask. Representatives might be able to take advantage of constituency alerting systems. News alerts about issues affecting their constituencies. Online opinion polling might help representatives "test the water" about potential policy decisions. Online voting might result.

And what of government itself? eGovernment? The UK already has an "Office of the e-Envoy" whose mission it states is to "ensure that the country, its citizens and its businesses derive maximum benefit from the knowledge economy". Will we eventually get that long sought after "joined-up government" via integrated databases?

The possibilities are, of course, endless. We need to start thinking about them though and what might go wrong as a result of these advances.

5.4 Assessment

End of Topic Test

Q1: Prior to the 1980s source code was always

a) Bug-ridden
b) Cheap
c) Made available
d) Written in Fortran

Q2: Linux is an example of

a) CSCW
b) Open source
c) Pervasive computing
d) Proprietary software

Q3: Which of the following is NOT permitted by copyleft?

a) Copying
b) Modifying
c) Running
d) Taking private

Q4: The licence which permits proprietary software to use open source library software is

a) Free Software Foundation
b) GNU General Public Licence
c) GNU Lesser General Public Licence
d) Open Source Definition

Q5: Which of the following phrases has been used to describe peer-to-peer?

a) Client/server
b) Cornucopia of the Commons
c) House of Commons
d) Tragedy of the Common Man

Q6: What societal concern was raised about advances in computer technology?

a) Exclusion
b) Piracy
c) Pornography
d) WiFi

Q7: Alienation was NOT suggested as a concern in the case of

a) Illiterate people
b) Innumerate people
c) People with special needs
d) Visitors from Mars

Q8: The Semantic Web was described as the World Wide Web in what form?

a) Hardcopy
b) Machine readable
c) Mobile phone
d) Ubiquitous

Q9: Pervasive computing was described as computers everywhere in what sense?

a) Background
b) Right here and now
c) Transparent
d) Virtual

Q10: When do we need to start thinking about what might go wrong?

a) Later
b) Now
c) Tomorrow
d) Yesterday

5.5 References

DiBona, C., Ockman, S. and Stone, M., 1999, *Open Sources: Voices from the Open Source Revolution.* O'Reilly.

Oram, A., 2001, *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* O'Reilly.

Raymond, E.S., 1999, *The Cathedral and the Bazaar.* O'Reilly.

Saha, D. and Mukherjee, A., 2003, "Pervasive Computing: A Paradigm for the 21st Century". *IEEE Computer*, March issue, pp. 25-31.

Sourceforge, 2005, *SourceForge.net: Welcome* [online]. 2005 [cited 24th July 2005]. HTML. Available from http://sourceforge.net/index.php

Williams, S., 2002, *Free as in Freedom: Richard Stallman's Crusade for Free Software.* O'Reilly.

Topic 6

3rd Stage Project Guide

Contents

6.1 Objectives

- To gain experience in planning and costing a substantial development project
- To gain experience in the specification, design, implementation and evaluation of a substantial piece of software
- To gain experience in developing marketing strategies for different types of enterprise
- To gain experience in documenting all of the above activities.

You are **not** expected to re-invent the wheel but make full use of the tools available on the computing platform you are using. If you feel you need facilities which are not available please consult your supervisor - he will be the final judge on whether your requests can be accommodated.

This Project provides coursework that covers material introduced across the three modules 'Tools and Methodologies 1 (F23HE)', 'Tools and Methodologies 2 (F23IA)' and 'Professional Development (F23HG)'. You will therefore find this Project Guide replicated as the final Topic in these three modules. Note that the Project is assessed as part of the Stage 3 'Computing' module set.

6.2 Organisation

Each student works under the direction of a member of staff. This member of staff is known as the *Supervisor*, and represents the immediate line manager of the student in a fictional software house where the work is being undertaken. The student is responsible for ensuring that deadlines are met, particularly with respect to document submission, and for maintaining a *Project Diary*.

Academically, all projects are overseen by the *Project Director*. The project director assigns students to projects and supervisors. Consultation time between the student and the supervisor should be about one hour per week.

The student, in consultation with the supervisor, is responsible for formulating the detailed requirements specification on the basis of the initial requirements. The supervisor is required to sign this document to indicate that both parties agree on what is to be developed.

6.3 Documentation

The *Project Diary* should be used to minute all meetings and who attended them and record all important decisions. It should contain **brief** summaries of all project meetings and of progress against the milestones laid out in the project plan. The diary should be submitted along with copies of all other documentation at the end of the project.

Throughout the year the student is required to produce a number of documents bundled into distinct *Deliverables* with associated deadlines. These deadlines are immutable.

Fanciful names for your software company are fine but all documents must be clearly labelled with the names of both the student and the supervisor. The contents of each document should normally be as described below.

6.3.1 Deliverable 1

This is to be produced by the end of **Week 6**. It should contain a *Requirements Specification* which has been signed off by the supervisor. A complete description of the project requirements and objectives should be specified either informally or using an appropriate specification formalism. An initial *Project Plan* should be provided, specifying intermediate goals and criteria, human resource allocations and estimated task completion times. A complete *Project Costing* should be included which justifies an overall budget for the project covering the costs of development, evaluation and marketing. Any additional costs for hardware, proprietary software, etc. should also be specified.

6.3.2 Deliverable 2

This should be completed by **Week 12**. It should contain a complete *Design* of the system to be implemented, including dataflow or class diagrams showing the relationship between system components, interface specifications for each system component and descriptions of input/output documents and files used by the system. It should also incorporate an *Implementation Plan* with a detailed chart of what will be done when and by whom. An *Evaluation Strategy* is also required which details how the system will be tested for technical correctness and assessed for fitness-for-purpose and usability. A *Marketing Strategy* for the fictional software house by whom the student and supervisor are employed should be specified. At the very least a *Website* should be designed.

6.3.3 Deliverable 3

This should be submitted by **Week 18**. It should include *Promotional Materials* in support of the marketing strategy. A *Prototype System* should be implemented by this deadline.

6.3.4 Deliverable 4

Week 25 is the final deadline for project completion. The final system along with the website for the software house should be completed by this deadline. Copies of all documents should be submitted in this deliverable. Documents submitted earlier in the year should be re-submitted as part of this complete bundle.

In addition the *Project Diary*, a *User Guide* and an *Evaluation Report* should be submitted along with an assessment of the project achievements measured against the initial requirements. The source code, test results and any similarly detailed material should appear as appendices, not in the main body of the report.

6.4 Resources

Database provision should use either Oracle or the Linux dbm routines.

HTML and web-based front ends can be used but must operate with the standard CGI-wrapper interfaces. NO private web servers will be set up.

Use of Rational Rose and similar design tools is welcomed but the code produced **must** compile and run on designated computing platform.

Requests to use any other resources must be supported by your suprvisor.

6.5 Demonstrations

One afternoon in **Week 26** will be set aside for all students to demonstrate their projects. This provides an opportunity for the student to display their work and compare it with that of others. Staff will also be able to get a feel for the general standard of projects.

At this time each student **must demonstrate their project to their supervisor and the project director**. This demonstration will form part of the assessment process.

6.6 Assessment

Assessment is based on the documentation submitted and on reports from the supervisor.

Interim feedback will be provided shortly after each deliverable has been submitted. This is for guidance only and will not form part of the final mark.

he supervisor and project director will return a Feedback Form for each project after the demonstration. All deliverables plus feedback forms are to be submitted to the Heriot Watt University for final assessment. Final assessment of the Project will be based upon the usual criteria for project assessment. These include quality and content of deliverables and final system, strategies adopted, planning, execution, demonstration of product, and organisation and management.

Answers to questions and activities

1 Professionalism

End of topic test (page 5)

Q1: c) Publicity

Q2: b) Industry advertisements

Q3: d) Plumber

Q4: c) Competence-Responsibility-Trust

Q5: b) Earning lots of money

Q6: c) Believing you are

Q7: b) 1957

Q8: d) Swindon

Q9: c) Practices specific to industrial functions

Q10: a) Giving value for money

2 Rights and Wrongs

End of Topic Test (page 15)

Q1: d) International Standards Organisation

Q2: c) TickIT

Q3: c) ISO 17799

Q4: d) Wrong

Q5: b) Look and feel

Q6: b) Longevity

Q7: b) Computer-based obscenity

Q8: a) Editing it

Q9: b) Plato

Q10: b) Golden Rule

3 Risks and Threats

End of Topic Test (page 27)

Q1: a) Debugging

Q2: c) Promiscuous

Q3: a) Deceit

Q4: c) Salami technique

Q5: b) Explosives

Q6: b) Digital signatures

Q7: a) Letter of recommendation

Q8: b) Involuntary

Q9: c) Hair colour

Q10: c) One

4 Dependence and Change

End of Topic Test (page 37)

Q1: b) Millennium bug

Q2: b) Direction

Q3: c) Fashion

Q4: b) Cooler

Q5: b) IBM

Q6: c) Moderate

Q7: c) 1996

Q8: c) Software

Q9: b) 1900

Q10: d) £300,000 million

5 Brave New Worlds

End of Topic Test (page 45)

Q1: c) Made available

Q2: c) Pervasive computing

Q3: d) Taking private

Q4: c) GNU Lesser General Public Licence

Q5: b) Cornucopia of the Commons

Q6: a) Exclusion

Q7: d) Visitors from Mars

Q8: b) Machine readable

Q9: b) Right here and now

Q10: b) Now