A2 MODULE 5 (ICT5) 14.5 NETWORKS

Network security, audit and accounting (Chapter 59)

- *Understand the particular security, audit and accounting problems associated with networks, and recall the steps, which can be taken to preserve security.*
- *Describe the measures taken to protect network traffic against illegal access.*
- *Understand the reasons for using audit software in providing a network service.*
- *Understand the reasons for using accounting software in providing a network service.*

Network environments (Chapter 59)

- *Understand how a network environment affects the user interface provided: security, control of software, control of files - access rights.*

Networking is linking as a series of points or nodes through telecommunications hardware, software and media to share resources and data.

Networks must: -
Generally organisations rank the following in order of importance

- Information must be accurate i.e. no data errors
- Information is **sent as quickly and cheaply** as possible.
- An organisation usually finds it pays to use the **fastest method** that you can keep busy.

Network OS must

- Identify each node
- Secure the attention of other nodes
- Deal with Error correction
- Keep records of traffic (Maintain an Audit and Transactions Log)
- Monitor security (Deal with passwords and access rights)
- Deal with Queuing (prioritise network activity)

Network Connection Software has certain functions

- Communications protocols
- LAN driver

A reliable network requires

- To be accessible when needed by users
- Not lose or corrupt data
- Be able to recover quickly from disasters such as power failure
- To be used by staff following codes of conduct
- Be regularly maintained and modified.

http://www.bcr.com/bcrmag/2002/06/p53.asp	Reliability
http://www.howstuffworks.com/firewall.htm	Firewalls
http://www.iacss.com/workshops.htm	Audit workshop
http://computer.howstuffworks.com/encryption.htm	Encryption
http://www.cit.cornell.edu/computer/responsible-use/	Code of conduct

A2 MODULE 5 (ICT5) 14.5 NETWORKS

Advantages from networks

- Be able to share software, hardware resources and data
- Access to data can be centrally controlled.
- Connect devices that would otherwise be incompatible
- Access services for security, user support, systems maintenance
- Expensive hardware resources and processing can be shared - e.g. expensive colour printer
- Only one copy of important data files required. Accessed by all and changes apparent to all users as they happen.
- Electronic communication is possible. Mail/messaging systems

By-products of networking are

- Improved operational efficiency, speed and accuracy
- Better control of resources (just-in-time)
- Improved productivity

General cautions and concerns noted by users

- Response Time is not always quick enough
- Reliability (excessive downtime in certain networks). It may not be possible to do anything at a local station if the network is down. Users may suffer unacceptable delays when the network is busy.
- Cost of installation and maintenance. A virus introduced at a single machine may quickly spread to all network stations.
- Problems with security.
- A network station can only be used where there is a network connection available
- Lack of standards – not fully open systems.
- Ethics - use by employees for non-business activities (code of conduct)

Security, audit and accounting (chapter 59)

The particular security and accounting problems associated with networks

Networks are extremely vulnerable to unauthorised access
Wide distribution - can be accessed by anyone in the world
Easy access to critical information opens new ways to alter or destroy and allow intruders access.
The volume of traffic needs
To be efficiently used

Networks provide particular security problems that are additional to those experienced by stand-alone systems.
A network is vulnerable to unauthorised access from any of the nodes that are attached.

Steps which can be taken to preserve security.

Train every employee about the company security policy **Heathcote P. 322**
Provide redundant file servers or disk drives

Firewalls – Heathcote Page 323

software that prevents unauthorised communications into or out of the network e.g. a proxy server that maintains replicated copies of Web pages for easy access by a designated class of users.

- Software that prevents unauthorised communication into or out of the network.
- The firewall is generally placed between internal LANs and WANs and external networks such as the Internet.
- Various different types are available, such as:
- Router - examines each incoming packet of data, checking its source or destination address. Access rules must identify every type of packet that the organisation does not want to admit;
- Special software that restricts traffic to a particular application such as e-mail or Lotus Notes groupware;
- A 'proxy server' - that maintains replicated copies of Web pages for easy access by a designated class of users.

Audit controls p. 323

Track all activity on a network – for example:

- What programs have been used;
- What files have been opened;
- How many reads and writes have been executed;
- How many times a server has been accessed.
- Monitoring software can be applied to the data that has been collected and possibly detect abnormal patterns of use and behaviour by users.

Lockouts (3 attempts only)

Encryption devices **Heathcote P. 300**

Prevents confidential data from being read by unauthorised hackers. Makes it incomprehensible to anyone who does not hold the 'key' to decode it.

- Methods include:
- transposition - characters switched around
- Substitution - characters replaced by other characters
- Cryptography serves 3 purposes:
- Helps to identify authentic users
- Prevents alteration of the message
- Prevents unauthorised users from reading the message

Documentation setting out disaster recovery techniques

Codes of Conduct/In-house standards

All employees:

- should be aware of the risks to data
- should follow rules and procedures
- be alert to possible security breaches
- be aware of potential dangers of internet access:
- downloading programs
- opening email attachments
- use virus protection software
- not leave terminal logged on when unattended

Performance Management **Heathcote P. 323**

Network monitoring software will collect data on:

- Network availability (i.e. switched on and not working);
- Response time (time between making a query and receiving a response);
- Utilisation of hardware resources (CPU, disks, bridges, repeaters, clients and servers);
- Utilisation of software;
- Traffic density in each segment of a network.
- This information can be used to identify bottlenecks and potential problems

It can also be used to plan future developments of the network

Backing up critical data (restore and recover)

Control access to workstations - see Access Privileges Heathcote P. 322

Have a hierarchical password system. This can be implemented by assigning users to groups. These groups can then be assigned particular access rights to directories or files. Typical access rights are:
Read - user can read data from the file but not changes it
Write - user can write data to the file
Scan - user can see the file name in a directory listing
Change - user can re-assign access rights
Create - user can create a new file in a directory

A group or an individual user can be granted one or more of these rights to any particular directory or file. In addition the network software can monitor the status of user passwords insisting on a change at particular time intervals, a minimum length and preventing re-use of old passwords.
Classify network users - user names, account numbers, passwords can be used to differentiate between authorised users and intruders. Thus important for users to keep this information confidential. (P.504)

Callback system Page 323

A network that involves remote access is particularly vulnerable to attacks by hackers. A dial back system in which the connection is established from the remote terminal for log in, broken, and the host computer dials the remote terminal back at the location associated with that user ensures that login in is taking place from the expected physical location. This method will not of course work with systems where a user cannot be identified with a particular location.

Keycards, fingerprints, voiceprints, retinal eye scans
File protection (read/write)
Virus protection

Access Controls

- May be based on:
- What you know
  password or PIN number - many shortcomings
- What you have
  ID card - smart card or magnetic stripe card
- Where you are
  access may be only from a specified location or phone number - callback system
- Who you are
  biometric identification by handprint, retinal image or voice print
- All methods are less effective if users are careless.
- Auto logoffs to try and counter carelessness

EXAM QUESTIONS

1997 (12 marks)

A university provides staff and students with access to its computer network.

a. Activity on the university's networking system is monitored and an accounting log is automatically produced. Suggest what this log might include and explain why it is useful. (8)

b. Appropriate staff have access to personal and financial data. What steps should be taken to preserve the security of the data in such a system? (4)

(a) What the log might contain: *Allow a 5-3 split in either direction*	
a record of facilities used by each person including processor time (1)	*no of pages printed (1)*
or disk space used (1)	*details of systems failures/ crashes (1)*
details files stored/ updated/deleted (1)	*details of e-mail usage/storage (1)*
time and duration of log-in (1)	*ID of logged in users (1)*
network address/station ID (1)	*failed log on attempts (1)*
Why it is Useful:	
provide systems administration with information about network load (1)	*enable administrators to deal with network performance problems (1)*
facilitate sensible distribution of resources to users (1)	*to limit use of scarce resources (1), possibly through a charging system (1)*
inform decisions about any upgrade or systems enhancement (1)	*dealing with network misuse (1)*
(b)	
allocation of hierarchical password to all (1)	*restricted physical access to hardware (1)*
different access rights for different users e.g. read only, read write (1)	*organisational codes of practice (1)*
restrict sensitive applications to certain terminals (1)	*staff training to raise awareness of security procedures/issues (1)*
existence of appropriate security procedures (1)	*audit of security procedures (1)*
auto-log off (1)	*restrict access to hard copies/printouts (1)*

1998.9 (20 marks)

An international company wants to set up a computer network. Although many staff currently use stand-alone desk-top systems the company has no experience of networking. As an IT consultant you have been asked to prepare a report for the company directors, outlining the issues, and the potential benefits, to communications and productivity that such a network could bring. Your report should include:

- a description of the various network components which would be involved:
- a description of the relative merits of different types of network which could be considered;
- a description of the security and accounting issues involved;
- an explanation of networked applications which could improve communications and productivity within the company.

A maximum of 6 marks is available for discussion of each area of the report. *Up to 4 marks are available for the quality and coherence of the candidate's argument. TOTAL 20.NB. Max Mark for content is 16/20.*
Max. 6: (Description of network components involved) (H)
In each of the following the mark is awarded for the name of the component together with a brief description of it's functionality.
Network cards in work stations to allow connection to cables (1), routers to link network segments together (1), switches (1), bridges (1), repeaters (1), types of network cable (thin Ethernet, cat5, atm, fibre optic, ISDN, etc) (1), servers (1), gateway (1), hub (1)
Max. 6: the relative merits of different types of networks which could be considered; (M)
Contrasting of LAN and WAN (2,1,0) – 1name = 1 mark
Different topologies exist examples of topologies e.g. ring, bus, star, peer-to-peer (2,1,0)
Relative merits of different topologies (2,1,0)
Need for routers, repeaters, bridges etc. (2,1,0)
Max. 6: the security and accounting issues involved; (S)
Need for hierarchical password system (2,1,0)
Different types of access can be allocated (2,1,0)
Accounting: recording/tracking which of users are logged-on (2,1,0)
Accounting: recording/tracking use of systems resources (2,1,0)
Need for organisational code of conduct (2,1,0) Etc.
Not data privacy and DP act
Max. 6: Networked- applications which could improve communications and productivity within the company (A)

Explanation of e-mail (2,1,0)	*Explanation of work-groups (2,1,0)*
Explanation of Intranet (2,1,0)	*Explanation of Internet (2,1,0)*
Distributed databases (2,1,0)	*Exposure to hacking/sparring (?) – firewall (2,1,0)*
Spread of virus, increased risk of exposure (2,1,0)	*Real Time Stock Control (2,1,0)*
Client server (2,1,0)	*EDI (2,1,0)*
Video conferencing explained (2,1.0)	*Real time stock control (2,1,0)*
EFTPOS (2,1,0)	*Etc.*

1999.4 (8 marks) The IT manager of a large college is about to change the software that is used to record student attendance in classes. Given that this new software must provide different access permissions and types of report, what capabilities and restrictions should the IT manager allocate in order to satisfy the needs of each of the following groups of users?

- students
- teaching staff
- office staff
- senior managers

Maximum 1 mark for each point for each user
Answers will depend on when and how attendance data is collected:-
•once per day via traditional registers which return to office for data entry,
• at each class, by swiping students id card in on-line reader,
• teachers with computers holding class lists with radio link to office for central upgrade/query, etc
NB. IF they say 'NO ACCESS for a user' = No marks for this part of the question.

Students

Read access only to attendance data (1)
Restricted to their own records (1)
May be able to give their own reasons for absence (1)

teaching staff:

read access only for a traditional method/central database (1)
may have write access for on-line method prior to upload to a central server (1)
search or query particular student records (1)
reporting at individual student level or class level or at department level or all records depending on the College (1)

office staff

input/edit and update capability (1)
restricted access to a departmental data set (1)
reporting at individual student level or class level (1)

senior managers

read only access (1) (Ignore read/write access here.)
access to full data set (1)
summary reporting rather than detail of each student or class (1)
If only 1 user is addressed- max 3/8
If only 2 users are addressed max 5/8
*Any 8*1= 8*

1999.6 (14 marks) A company has a computer network system.

(a) Activity on the network system is monitored and an accounting log is automatically produced.
(i) State **four** items of information that this log might include. (4)
(ii) Give **four** reasons why such a log is useful. (4)
(b) An IT consultant has suggested that the company changes from a peer-to-peer network to a server based network. Give **six** features of these network environments, which contrast the two different approaches. (6)

(a)** (i) **What the log might contain: maximum 4 from:

a record of facilities used by each person including processor time(1),	*no of pages printed (1)*
or disk space used (1).	*details files stored/ updated/deleted (1)*
details of systems failures/ crashes/error messages (1)	*details of e-mail usage/storage (1)*
IDs of logged-on users/who (1)	*time & duration of log in/log out/ when logged in (1)*
network address/hardware id of logged on users/details of workstations (1)	*details of applications used/count of users per application/ no. of licenses used (1)*
details of network traffic (1)	*details of failed login attempts (1*
4x1=4	

*(ii) **Why it is useful:** (Max. 4 from)*

provide systems administration with information about network load (1)	*monitoring software licenses (1)*
enable administrators to deal with network performance problems (1)	*facilitate sensible distribution of resources to users (1) e.g.. memory/time/printers/ etc.*
to limit use of scarce resources (1), possibly through a charging system (1)	*inform decisions about any upgrade or systems enhancement (1)*
help in controlling abuse of network (1)	*enable administrator to identify and support novice users (1)*

(b)

Central or main computer exists on server based network but not on peer-to-peer (1)
Shared data/programs/applications stored on server c/w on any local hard drive (1)
maintenance benefit of installing applications once on server c/w installing copy on each local hard- drive in peer-peer (1)
systems manager overheads for a server based network (1) E.g. setting up user accounts and access rights. (1)
shared resources such as printers, hard drives, etc in peer-peer only available when workstation is on c/w available when network is up for server based (1)
Server based net can simplify job of central administrator, at some cost in performance (1)
Server introduces single point of failure (1)
Server implies one 'more capable' machine suited to serving many clients. (1)
server based network tend to be much larger scale than peer-peer (1)
software upgrades more easily managed on server based network (1)
security issues harder to control on peer-peer (1)
server based nets likely to need additional hardware: routers, bridges, repeaters, switches, etc (1)
centrally managed backup on server based net. (1)
speed of access varies with number of users/load on server based net. (1).

General answers about speed of access score 0.
Do not credit answers about topology – e.g. peer-peer : when one station crashes, the whole network crashes.
Do not credit answers about software licenses -e.g. claims of need to only buy one license for server.
Any 6x1=6 Total 14

1997 (8)

A hospital information system holds program files, which are rarely changed, and large database files, which are constantly changing.

Describe a suitable backup strategy for this system, explaining what is backed up and when, together with the media and hardware involved.

Max. 8: candidates must address both types of file. Max. 5 for any area.

Database files:

Strategy:	*recognising need for rapid recovery (1)*
mention of incremental dumping (1)	*use of bypass systems so that processing can continue if main computer fails- (1)*
through use of intelligent terminals with local hard drives (1)	*possibility of transaction tracking where all transactions are logged (1) due to possible loss of alterations between incremental dumps (1)*
generation systems (1)	
When*:*	*during a terminal session all updated files are marked (1).*
and when user logs out these are dumped to disk (1)	*need to shut down to back up (1)*
May be dumped more frequently while user is working (1).	

Media & Hardware*:*

mirrored disks on servers (1)	*DAT/tape/exchangeable disk packing*

Program files:

Strategy:

periodic dump to tape (1)	*generations system (1)*
may need to shut down systems to backup/use bypass facility (1)	*backup process may be time consuming. (1)*

When:

backup prior to systems maintenance (1)	*backup prior to upgrade (1)*

Media Hardware:

tape , changeable disk packs	*(1) NOT - re-install from distribution disks*
NOT answers based on floppy	

June 2002.3

Networks of computers are rapidly becoming part of everyday life, both for organisations and individuals. Communication over networks involves the use of protocols.

a. Define the term protocol. (1 mark)

b. With the aid and an example, describe **one** advantage of using protocols.(3 marks)

c. State **one** consideration that should be taken into account when setting up a network, and explain why it is important. (2 marks)

a. A standard set of rules that define how communication will take place between computers (1) or any acceptable definition

Max 1

b. Users are not restricted to one manufacturer's equipment / allows for the existence of open systems (1) meaning several disparate pieces of equipment can be connected together and can be expected to communicate effectively (1) + a relevant example (1)

Max (3, 2, 1, 0)

c.

- *Previously installed network devices/ software need to be considered (1) to avoid address conflicts (1) OR device addresses need to be unique (1) so that each device is uniquely identified on the network (1)*
- *Network Operating System has to be considered (1) so that correct protocols are set up (1)*
- *How devices are connected to the network (1) it may cause a bottleneck and so there may be congestion (1)*
- *If the devices are set up to access the Internet (1) they will have to use TCP/IP to communicate (1)*
- *Applications will need to use the correct protocols (1) e.g. different e-mail servers use different settings (or other relevant example) (1)*
- *Size of network (1) + expansion (1)*
- *Security issues (1) data on the network may need to be protected/ have restricted access (1)*
- *Network usage (1) + expansion (1)*
- *Max (2, 1, 0) 6 marks*

June 2002.8

a. Describe **two** changes that may be evident to end-users when they change over from using a stand-alone computer to a networked environment. (4 marks)

b. A multinational company has recently created an Intranet, connecting all of its computer systems.

All its sites are now connected using high-speed dedicated links.

i. Describe **one** facility that could now could be made available to the company which would improve productivity. (2 marks)

ii. Describe **two** possible problems that may arise as a result of using this network of computer systems. (4 marks)

iii. Describe **two** possible measures that the company can take to combat problems caused by the use of this type of network. (4 marks)

a.

- *login screen (1) user now has one more stage to complete before they are able to use their system (1)*
- *more disk drives on screen (1) user now has access to drives that are logical rather than physical (1)*
- *less control over data (1) user may now find that they have changed / no right to access files they could previously (1)*
- *physical appearance of workstation / environment (1) for example extra ports on*
- *machine / extra cable connected to machine / ability to print to other machines / extra hardware in the form of hubs etc (1)*
- *access to remote/ shared resources (1) + expansion (1)*
- *less control over the interface (1) e.g. inability to customise (1)*
- *increased communication using / via the machine (1) + example (1)*
- *references to 'transfer of personal settings' can be awarded as a BOD (1)*

b.

i.

- *Video-conferencing (1) managers will be able to see each other without the need for travel costs/long arrangement times (1)*

- *Group working on projects using productivity (1) work can be completed in a shorter time scale (1)*
- *Distributed databases (1) meaning that all users have access to the same information all the time / changes are reflected everywhere as soon as they are made (1)*
- *Electronic sharing of documents (1) means that there is less reliance on physical media (1)*
- *Ability to share hardware resources (1) means that funds can be devoted to other areas of the business/less hardware needs to be purchased/excess hardware can be sold off (1)*
- *e-mail (1) which means you have more control over spam / viruses/ etc. (1) OR internal e-mail (2)*

DO NOT ACCEPT INTERNET ACCESS. DO NOT CREDIT BRAND NAMES.

ii.

- *risk of unauthorised access (1) meaning potentially sensitive/confidential information may be accessible (1)*
- *risk of viruses (1) all nodes need to have up to date anti-virus software (1)*
- *reliance on external agencies (1) e.g. the telecommunications network that the company has little/no control over (1)*
- *more vulnerable to spurious data (1) if incorrect data is entered into the system, the mistake may not be picked up for a long time (1)*
- *more difficult to back up (1) as there will be no one centralised control (1)*
- *increased management overhead (1) means that more time/money/manpower will*
- *need to be dedicated to the computer systems (1)*

DO NOT CREDIT THE TERM HACKER UNLESS IT IS SUPPORTED BY AN EXPLANATION

iii.

- *Provide user login and password (1) to make it more difficult to enter the system if not authorised (1)*
- *set up required procedures (1) so that users know the tasks that need to be carried out to maintain system security/integrity (1)*
- *invest in redundant systems for mission critical applications (1) so that if disaster hits, essential business functions can still be carried out (1) . ensure validation/verification checks are made on data (1)*
- *encryption of data (1) so that intercepted datal packets cannot be understood (1)*
- *use up to date anti-virus software (1) + expansion/ example (1)*
- *use a firewall (1) e.g. to provide a filter on traffic coming in/ going out (1)*

June 2002.9

A local council has decided to standardise the ICT systems across all its departments. This is due to problems experienced in transferring data and staff between departments.

Discuss the above statement. Include in your discussion:

- the benefits that the staff may gain from this approach;
- the benefits that the council may gain from this approach;
- the reasons why staff may not wish to change.

The quality of language will be assessed in your answer. (20 marks)

(qu 9 ICT5)

Allocation of marks:

- *Up to 6 marks for benefits to staff (code as S)*
- *Up to 6 marks for benefits to the council (code as C)*
- *Up to 6 marks for why staff may be resistant to change (code as R)*

For each section, award marks for up to 3 points, i.e. the second mark each time is gained by expanding upon a specific point. Reasons must relate to points given.
Maximum mark for content is 16/20. Up to 4 marks are available for the assessment of Quality of Written Communication (code as Q).
BENEFITS TO STAFF (S marks)

- *ease of learning (1) the council can produce standard training documentation that matches the workstation HCI (1)*
- *easier transfer of skills (1) due to consistency of interface (1)*
- *user can make use of other workstations (1) so user does not have to be fixed to one work area (1)*
- *users are able to support each other (1) meaning simple problems can usually be solved without recourse to user support (1)*
- *standard setting of defaults (1) e.g. word processing package can be set with standard margins to suit the standard printer (1)*
- *easier distribution/use of standard items (1) such as logos/templates/etc (1)*
- *etc.*

BENEFITS TO COUNCIL (C marks)

- *less training overhead (1) as everyone can attend the same training (1)*
- *perceived image of council may improve (1) as anything produced will now definitely be in the required style (1)*
- *easier quality control (1) as there are less things to go wrong if everything is done in a standard way (1)*
- *easier to manage licensing (1) as all workstations should have identical software content (1)*
- *upgrades will be easier to administer (1) - there is less management*
- *security is easier to monitor (1) it will be more obvious is a workstation has had its contents altered (1)*
- *etc.*

RESISTANCE TO CHANGE (R marks)

- *consideration of skill level of user (1) standard will only suit a certain cohort of users/it may be too low level for experts or too high level for novices (1)*
- *less control over software (1) user has to wait for software configuration to be changed for them rather than do it themselves (1)*
- *availability of specific software (1) unless software is standard, user may lose necessary functionality (1)*
- *'special needs' consideration (1) colour sets may not suit colour blind*
- *users/physical workstations may preclude use by those with other disabilities (1)*
- *original system served user perfectly well (1) so user cannot see the point in changing/sees this as a waste of their time (1)*
- *etc.*

Spring 2003.5

Whilst planning to install a network accounting system, a company has become concerned about the security of its local computer network.

a. Explain two procedures that the company could adopt to discourage breaches of security. (6 marks)

b. State two reasons for using accounting software on a network. (2 marks)

a.

- *Procedures for employing/ vetting staff (3,2,1,0)*
- *Procedures for restricting' controlling system access (3,2,1,0)*
- *Procedures for use of information gained from network accounting/ auditing systems (3,2,1,0)*
- *Procedures for the use of removable media (3,2,1,0)*

Credit any point that relates to company issues and that can justifiably form part of a code of practice.

Marks can allocated for: What is the procedure (I), expansion (1) why is it an appropriate procedure for the company (1)

NB The question is about procedures

b.

- *Charge users for use of scarce/expensive resources e.g. colour printing (1)*
- *See where network has high traffic in terms of time or location so that it can be dealt with/ charges adjusted accordingly (1)*
- *To ensure that resources are being utilised efficiently (1)*
- *Encourage efficient use of resources (1)*
- *Able to vary charges with respect to requirement and/ or utilisation (1)*

June 2003.*4*

A large international corporation uses an extensive wide area network, linking all its offices around the world to exchange data and information.

Describe **four** ways in which the company can use its computer network to support the exchange of data and information. *(8 marks)*

June 2003.5 A travel company is reviewing the current disaster recovery plan for its computer-based booking system. Bookings come into the company by various means, including via post, over the telephone and via the Internet.

a. State, with a different reason for each one, **three** possible weak points in the booking system. *(6 marks)*
b. Besides the frequency and content of the backups, and the media used, describe **two** other issues that should be considered when reviewing the backup strategy. *(4 marks)*