Chapter 4 TECHNICAL OPERATIONS

This chapter discusses the management and the use of safeguards incorporated in ICT assets and other related devices. This chapter seek to explain in more detail the various option available that could be use to further enhance the management of ICT security. It covers the various aspects of computer systems, operating systems, application systems and network systems.

4.1 Computer Systems

ICT assets component

As defined in the Public Sector ICT Security Policy Framework, the ICT asset component comprises of information processing facilities such as mainframes, minicomputers, microcomputers, laptops, notebooks, palmtops, servers, workstations, departmental, corporate and personal computers as well as communication facilities and network equipment such as the facsimile, fixed line telephones, mobile telephone systems, power supplies, environmental control units, routers, bridges, switches, computer and communication hardware and software, utility programs, operating systems, documentation and applications software. The housing facility is also part and parcel of the public sector ICT asset. With regard to the ICT security of these systems and sub-systems, the following controls need to be exercised:

4.1.1 Change Control

Change control procedure should exist for hardware, software, manual procedure and emergency changes

Change Control can be defined as the processes initiated to manage and control planned changes about to occur and that the changes will affect ICT operations or its environment. The triggering Change Control events may be scheduled or in response to an emergency. ICT being volatile, Change Control is necessary to protect the integrity of information processing systems and should exist to meet changes in hardware configuration, software changes, manual procedure changes or other changes that will affect service delivery.

Establish effective change control procedure

Change control is established to ensure smooth migration and minimal operational disturbance. As such, it should be well thought off and effective. Change control should consist of at least the followings:

(a) formal change request;

(b) formal authorisation process;

(c) test and system acceptance procedure for every change to consist at least unit test, component test and integration test;

(d) fully documented changes and expected outcome;

(e) virus checks before and after changes are made, where appropriate;

(f) back-up and restore procedures to capture the system image prior to the new environment; and

(g) explanatory exercise for user buy-in.

4.1.2 Equipment Maintenance

Equipment under maintenance or scheduled for maintenance can be a vulnerability source. To ensure the integrity of equipment, implement the following security controls:

(a) ensure correct equipment is sent for maintenance and that maintenance is due or necessary;

(b) maintenance conducted by authorized personnel;

(c) remove sensitive information if possible;

(d) equipment containing sensitive information when under maintenance should be supervised;

(e) inspect and test equipment before and after maintenance;

(f) record all faults and detail of repairs; and

(g) virus checks before and after maintenance, where appropriate.

4.1.3 Disposal of Equipment

To prevent inadvertent disclosure through disposal of equipment conduct the following:

Ensure sensitive information in equipment to be disposed is properly erased

(a) erase or destroy all information regardless of sensitivity and perform confirmation. In some instances, it may be necessary to destroy the equipment; and

(b) record all disposal and method used to erase or destroy the information.

4.2 Operating systems

Secure operating systems tested against security standard such as TCSEC

There are various categories of operating systems. The most secure operating system tends to be very close and proprietary and the least secure are more open and known to many. The security level of operating systems is categorised based on well-known security standard such as the Trusted Computer Security Evaluation Criteria (TCSEC) also known as 'The Orange Book' and the Common Criteria (CC).

Rahsia and *Rahsia* Besar should reside on trusted OS equivalent to a B1 security level or above

It is advisable that all government computers handling *Rahsia* and *Rahsia Besar* information use trusted operating systems certified to a level equivalent to or above B1 Security of TCSEC.

Only authorised system administrator should be allowed to access host OS

Due to the fact that the operating system controls all applications running on the computer and most technical staff is capable of manipulating the operating controls, it is therefore prudent to prevent intentional or inadvertent security breaches through the operating system. If possible, all changes to the operating system should acquire prior approval and later be monitored by knowledgeable security and audit personnel. An essential rule is to disallow technical staff other than authorised system administrators to operate a mainframe, minicomputer, desktop server or have access to its operating system. Where this is not feasible, close supervision is imperative.

4.2.1 Proprietary Issues

Need to balance between security and openness

ICT Managers and planners should have in-depth knowledge and understanding of the implication of choosing specific operating systems and their impact on the legacy and future systems. As much as possible, the public sector should remain with the non-proprietary operating system to eliminate the unnecessary cost of maintenance except in instances where high security is needed.

The right balance between security and openness must be properly defined by the assistance of security specialists and to take into consideration the business needs against serious implications.

4.2.2 Shareware and Freeware Operating System Issues

The use of shareware and freeware operating system should be carefully considered. Any downloaded shareware or freeware may contain malicious code that pose a threat to the security system of the organisation.

Downloaded shareware or freeware should not be used to process government data because this may cause spreading of malicious code. If unavoidable the shareware or freeware must be screened against such code before being installed.

4.2.3 Logical Access Control

Access control is essential to prevent unauthorised access and provide fast access failure reporting

This is a set of controls employed at ICT installations aimed at permitting only authorised access and providing fast access failure reporting. Some of the access control mechanisms employed is described below:

The materials can be used to formulate departmental access control policy. The ICTSO has to decide which is mandatory, optional or conditional.

4.2.3.1 Identification of Users

Steps to ensure only legitimate users use the system

Users of ICT systems can be an individual or a group of users sharing the same grouped user account. In both circumstances, users should assume responsibility for the security of the ICT system they are using. Some of the steps undertaken to positively identify legitimate users of the ICT system are:

(a) assign a unique user ID to each individual user. It is best to consult the user on the actual ID to be used rather than assigning a pre-determined user ID. In other words allow the flexibility for the user to choose his or her own ID or provide the ability to change the ID on first use;

(b) hold each and every individual accountable for all activities under the registered user ID;

(c) ensure that there are auditing facilities to trace all user activities; and

(d) ascertain that all user IDs are created upon legitimate departmental request and leave no opportunity to create unneeded user IDs.

In ensuring that unused user IDs (example due to long leave, attending courses, etc) are not misused:

(a) suspend all user privileges after 30 days of non-use and delete after 30 days suspension; and

(b) revoke immediately all privileges of users who have been re-assigned, transferred or terminated.

The system administrator should be informed on occasions where users are away from the office for a duration of more than seven (7) days so as to enable periodic monitoring.

It is good practice to archive audit trails of user activities

It is possible that security incursions might have occurred in the past without being detected. Therefore it is good practice to archive audit trails of user activities. However, the down side of such activity is storage requirement. It is recommended that activities of users who have access to sensitive information be archived.

4.2.3.2 Authentication of Users

Authentication is normally by passwords

One of the salient principles of ICT security is the authentication process that confirms the validity of the user or point of origin of the communication through the use of passwords. It is further strengthened by controls such as the requirement for all users to make immediate reports in cases of lost, compromised, suspected loss or suspected compromised passwords.

In order to minimise password disclosure:

(a) passwords should be entered in a non-display field;

(b) be of minimum length of eight (8) characters;

(c) require and enforce that passwords be changed at least once in 30 days;

(d) make available distress passwords for sensitive operations (a distress password is different from the normal user password and is used as a pre-arranged signal to indicate duress or coercion);

(e) passwords shall not be shared or made known to others, including administrators;

(f) instruct users not to use easily guessed passwords, i.e., own names, phone numbers, date of births, common words or numbers;

(g) use combinations of both alphabets and numeric characters;

(h) all passwords should be memorised and be stored in a secured location if required to be written down;

(i) encrypt password during transmission, where possible;

(j) store password files separately from the main system application data;

(k) prevent reuse of the user's last four (4) passwords;

(l) prohibit the display of passwords on input, reports, or other media; and

(m) one time password - the generation of new passwords for each session using pre-determined information that the user possesses or knows.

Proper authentication through use of dynamic passwords can be assured by implementing some of the following measures:

(a) selecting authentication tokens that are user changeable or activated by biometrics data;

(b) prohibiting the sharing of token PINs;

(c) ensuring that security tokens are resistant to tampering and duplication;

(d) using a different PIN from the user ID;

(e) using the PIN of minimum eight (8) length characters;

(f) randomly generated passwords to be used only once;

(g) encrypting keys and other information critical to authentication within the token and on the validating system;

(h) locking access after three (3) invalid tries;

(i) maintaining an inventory control on security tokens;

(j) requiring employees to acknowledge receipt of security tokens and explain conditions of use together with consequences of misuse;

(k) taking steps to recover immediately dynamic tokens from the employee upon reassignment or termination and terminate access privileges associated with the token assigned to the employee;

(l) conducting one-time challenge i.e. the ICT system challenges the authentication of the user when users log-on. To provide the answer, a specialised (hand-held) device would normally be used where upon input of the challenge, the authentication code is revealed. The user then proceeds to submit the authentication code. The authentication code is only used once and not repeated;

(m) using the digital certificate and electronic signature i.e. the use of a trusted third party appointed by the government; and

(n) using Biometrics or the process of using a unique attribute held by the person as a means of identifying that person including fingerprints, iris patterns, voice, face geometry, the shape and size of hands and fingers etc.

4.2.3.3 Limiting Log-on Attempts

Maximum logging attempts limited to 3

It is recommended that log-on be limited to three (3) attempts. The user ID should be suspended after the maximum of three consecutive unsuccessful log-on attempts. To begin investigation of attempted log-on, use the information detailing the attempted log-on as a reference point. The legitimate user should also be informed of such attempts.

Where authentication is used, there should be a time limit to verify the authentication. It is suggested that the authentication time limit be set to two (2) minutes (depending on organisation or location of logging-on) upon which the session is terminated.

4.2.3.4 Unattended Terminals

Ensure safety procedures are carried out on unattended terminals

In order to prevent unauthorised use of unattended terminals connected live to a system:

(a) activate the authentication process after a 10 minutes lapse of inactivity before allowing work to continue;

(b) activate a one-button lockup or initiate shut-down sequence when terminal is inactive;

(c) avoid storing passwords or any information that can be used to gain access on workstations; and

(d) implement password screen saver.

4.2.3.5 Warning Messages

Display warning against unauthorised access clearly

It is recommended that all users be reminded of their accountability when accessing ICT resources. This could be done, prior to log-on, by displaying a warning against unauthorised access or improper use and the consequences for such activity.

4.2.4 Audit Trails

Audit trails are records useful in events of mishaps

Audit trails are records of activities used to provide a means of restructuring events and establishing accountability. The audit trail information is essential in an investigation when problems occur.

Provide an audit trail for computer systems and manual operations when:

(a) critical information is accessed;

(b) network services are accessed; and

(c) special privileges or authorities are used, such as, security administration commands, emergency user IDs, supervisory functions, and overrides of normal processing flow.

Include in the audit trail as much of the following as is practical:

(a) user identification;

(b) functions, resources, and information used or changed;

(c) date and time stamp;

(d) workstation address and network connectivity path; and

(e) specific transaction or programme executed.

Provide additional alarm for security related events

Provide, where practical, an additional real-time alarm for significant security-related events such as:

(a) access attempts that violate the access control rules;

(b) attempts to access functions or information not authorised;

(c) concurrent log-on attempts; and

(d) security profile changes.

In such cases:

(a) investigate and report suspicious activity immediately;

(b) ensure that System Administrator reviews the audit trail information on a timely basis, usually daily;

(c) investigate and report security exceptions and unusual occurrences;

(d) retain the audit trail information for an appropriate period of time for business requirements; and

(e) protect audit trail information from deletion, modification, fabrication or re-sequencing, by use of Machine Access Control (MAC) or digital signature.

4.2.5 Back-up

In order to ensure that the system can be recovered in the event of a disaster, regular back-up should also be done whenever the configuration of an operating system is changed. This back-up must be kept in a secure environment.

When doing back-up, consider:

(a) document back-up/restore procedures;

(b) keeping three (3) generation of back-ups;

(c) keep back-up copies off site; and

(d) test back-up media and restore procedures.

4.2.6 Maintenance

In order to maintain, the integrity of the operating system against security breaches and vulnerabilities, employ the following controls:

4.2.6.1 Patches and Vulnerabilities

New vulnerabilities and bugs are constantly being discovered and once discovered they are broadcast and released by authorised security agencies such as Malaysian Computer Emergency Response Team (MyCERT), Canadian Computer Emergency Response Team (CCERT) or Australian Computer Emergency Response Team (AusCERT) as well as software providers like Microsoft. It is the role of the ICTSO or System Administrator to be aware and keep abreast of this development issued by Government Computer Emergency Response Team (GCERT) and implement the suggestions.

4.2.6.2 Upgrades

Procedures should be established to maintain the most current version of the operating system. However the decision to upgrade to the latest version need to be evaluated based on its implication to the overall system operation as well as cost incurred.

4.3 Application System

Public sector uses both commercial and internally developed software

Within the public sector a mixture of commercially and internally developed application software have been installed and are in use. In general, all access to software must always be justified and authorised.

The following controls should be implemented for the protection of software and the information that it processes:

4.3.1 Application Software

Implement ICT security control within applications

Within the application of the software, ICT security control should be implemented to prevent unauthorised access, modification, disclosure, or destruction of information. Some of the controls include:

(a) an integrated system security with an operating system access control facility, that allows for centralised and standardised user ID and password management;

(b) an established access profile structure that controls access to information and functions based on need-to-access requirement;

(c) consistent access controls on information that is replicated on multiple platforms. For example if a person is allowed to have read access to information in a certain operating system (e.g. Windows), this read access right applies to the other operating system (e.g. UNIX);

(d) an application control that identifies specific accountability of a user using a user ID. All transaction details should at least be logged with a user ID, showing time, date and activity;

(e) an information ownership incorporated system, where ownership may be accountability on a group or individual level;

(f) an application of the location control method that restricts access at specified locations or areas;

(g) dual control capabilities for identified critical transactions. Example: the requirement to have two (2) persons holding a user ID and password to transact monetary movement; and

(h) immediate logging and report of violation messages in case of occurance.

4.3.2 Databases

Databases need to be protected from unauthorised access

Controls should be implemented to protect databases from unauthorised modification or destruction. The integrity of information stored in databases can be maintained through the following:

(a) a database management system that ensures the integrity of updating and retrieval of information. Concurrent control is required for user-shared databases;

(b) a controlled access to information specified by either System Administrator, ICTSO or CIO; and

(c) an access control mechanism to physical information resources to restrict access to authorised information management systems, applications and users.

4.3.3 Systems which Employ Artificial Intelligence

Security controls should be included in AI based application system

Applications using artificial intelligent (AI) techniques such as automatic decision-making should include controls specific to that technology as follows:

(a) secure knowledge bases used by inference engines or similar AI processing techniques as well as a regular review for accuracy and effectiveness;

(b) set a maximum limit on automatic decision making ability of AI systems or AI sub-systems of conventional applications to ensure that unexpected errors of failures can be determined;

(c) an AI system which is used to make highly sensitive decision must not be set in a totally automated mode. Instead it should act in an interactive mode with humans to ensure that vital decisions are approved;

(d) set controls on information used in training of neural networks based applications;

(e) monitor the stability of neural network based-applications for effectiveness; and

(f) build all AI systems within programmed decision enclosures to ensure that the control of decision-making is kept within reasonable limits according to the information being processed.

4.3.4 Application Testing

Testing to ensure applications function according to specifications

One aspect of application systems development using the Software Development Life Cycle (SDLC) methodology is that of testing, which is required during the final stage of development. It involves the testing of a newly acquired application, upgrading an application or migration from old to new hardware. This is required to ensure that systems are working according to specifications.

Protect data during testing

In order to protect information from disclosure or inappropriate processing during application testing:

(a) use dummy or historical data for testing purposes;

(b) establish a policy that controls the use of classified information during application testing and use access control to limit access to appropriate personnel only;

(c) dispose of information used in the system during testing (especially when using the historical data); and

(d) require the use of physically separate environments for operational and development systems. This can be applied by establishing a development environment for the developers to design, develop, test and integrate the application systems.

4.3.5 Defective and Malicious Software

Internally developed or outsourced software could be defective

Development of software can be categorised into two (2) types: internal development or outsourcing. Both cases will encounter the defective software. In most cases the defect will be determined during the testing stage.

However, to minimise the probability of latent defects in software, controls should be properly implemented as follows:

(a) require the software acquisition system to select vendors with a good reputation, a proven record and sufficient resources. This is an important criterion to minimise the possibility of the supply of defective software. It will also improve the level of confidence in the acquisition of the software;

(b) establish a quality assurance programme and the procedure for all software developed internally or acquired externally;

(c) require that all software be fully documented, tested and verified to its maturity, robustness and effectiveness; and

(d) if it is discovered in the future that the software provider has inadvertently included malicious code into the software system (e.g. system may be used for international espionage or intelligence gathering on government information) then a liability clause must be included in the contract.

Users are required to report defective or malicious software to the helpdesk.

4.3.6 Change of Versions

Control and maintain integrity of software with new versions and upgrades

Software (application, OS, utilities, tools) is upgraded regularly. New versions are issued to ensure it is bug free and to upgrade functionalities. However changing of software versions should be controlled to maintain the integrity of the software when changes are made and this requires change control procedures to be followed [Refer to 4.1.1 Change Control].

4.3.7 Availability of Source Code

Consider escrow agreement for purchased software for which source code is not available

If the software system were developed internally, the source code would be easily available. However, if the system is purchased off the shelf, most vendors do not supply the source code to their customers. In order to ensure that source code is available for debugging or enhancement, controls should include the following:

(a) establish procedures to maintain the most current version of programmes written; and

(b) consider an escrow agreement for purchased software for which source code is not available in the event of disaster or national security breach.

4.3.8 Unlicensed Software

Unlicensed software is illegal

Unlicensed software is illegal. The Malaysian Copyright (Amendment) Act 1997 specifically prohibits the use of unlicensed software. The Ministry of Domestic Trade and Consumer Affairs enforces this Act and monitors the use of unlicensed software.

Usage of licensed software means software for which a license has been issued and control of inventory such as the safe keeping of the license. The inventory includes the physical control of the location of the licensed software and a copy of the license issued.

4.3.9 Intellectual Property Rights

IP rights for developed software should be specified in the contract

The Intellectual Property (IP) right is the right to claim ownership of a document, software or other creation.

Commercial software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only.

In order to prevent infringement of intellectual copyrights due to unauthorised copying of software on mass storage media, compliance to the Malaysian Copyright (Amendment) Act 1997 must be ensured at all times.

It is recommended that the IP rights for in-house or jointly developed software be specified in the contract.

4.3.10 Malicious Code

In order to maintain the integrity of information and protect it from disclosure or destruction from malicious code such as viruses, Trojans or worms, the following controls should be applied:

(a) install a system and implement a procedure to manage malicious code. All software acquired should be screened for such code prior to installation and use;

(b) establish a written policy on downloading, acceptance and use of freeware and shareware;

(c) authenticate software for applications using MAC or digital signature. Failure to verify indicates a potential problem and all use of the software should be halted;

(d) distribute instructions on the detection of malicious code to all users;

(e) establish a policy and procedure for the checking of diskettes; and

(f) seek assistance in case of suspected infection. Assistance may be sought from internal technical staff and/or vendors.

In ensuring recovery of processing capability following a malicious code attack, certain steps need to be performed including the following:

(a) retain an original back-up copy of all software, data and information for the purpose of restoration; and

(b) ensure that all data are backed up regularly.

In the case of virus infection, the following steps are recommended:

(a) use the approved virus application software;

(b) scan the virus using the facility from the software;

(c) delete and/or remove the virus immediately; and

(d) check the status of the scanning from the software report log.

4.3.11 Unauthorised Memory Resident Programs

Perform periodic inspection of installed software

Memory Resident Program (MRP) is a program that is loaded into memory where it remains after it finishes its task, until it is explicitly removed or until the computer is turned off or reset. The program can be invoked again and

again by the users (with the aid of a hot key) or by an application. In order to prevent unauthorised MRP, for example those that allow seemingly normal processing to take place but retain ultimate control over functions of the processing resource, perform periodic inspection of software installed to ascertain whether any unauthorised software has been inserted:

(a) implement additional controls (based on business needs) such as, token-based authentication devices, security modems that can provide password and dial-back controls or remote computing software that can provide password controls; and

(b) use secure remote access approved equipment.

4.3.12 Software Provided to External Parties

Secure a dedicated environment for software or insist on written statement from vendors

There may be cases where software is provided by government to external parties such as a private company owned by the government. In order to prevent unauthorised destruction or modification of such software, the following controls should be implemented:

(a) create and secure a dedicated environment for diskettes, CDs or other storage media. This should include physical and logical controls on the hardware, software and diskettes used for creation, copying, and protection; and

(b) require a written statement from distributors of software against malicious code.

In order to protect the public sector against claims of negligence due to the use of provided software, ensure the following controls:

(a) execute an agreement with external parties to whom software is provided that enumerates each party's responsibilities, required security duties and limits on liability; and

(b) maintain sufficient documentation to prove that the provided software was not the cause of viruses or other malicious code.

4.3.13 Software from External Sources

Prevent introduction of unauthorised software from external sources into the system

Care should be taken to prevent software being introduced into the domain through software downloading facility without the specific request or consent of the department. As an example, software providers will often download software to their customers. Another example is the downloading facility set up by vendors to distribute the latest version of the software.

In order to prevent unauthorised software from appearing in the system include the following:

(a) establish procedures on the downloading of software from external sources;

(b) organise a mechanism where downloaded software can be distributed into a server in a demilitarised zone (DMZ) to be accessed by a System Administrator later; and

(c) require the firewall to include virus scanning or ensure that any executable file is scanned for viruses before it is introduced into the network.

4.4 Network System

Measures to protect network equipment

A network is a system, which interconnects a multitude of computers and workstations for the purpose of communications and information/resource sharing. In keeping the various interconnected parts of the system interoperable, rules and procedures must be established. In a secure processing environment, networks have additional 'layers' of rules and procedures imposed, each addressing unique security requirements, with no one set of requirements (software or hardware) applicable to all security issues for any specific situation.

Problems could occur because there are layers of security, each very narrowly focused for specific conditions. In case of ever emerging systems and new equipment with greater capabilities and a multitude of abbreviations and operating names, 'old' rules can be easily forgotten in favour of simple ways of dealing with security, regardless of the layers involved. This tendency has created both the need for increased understanding of the various security layers when using shared resources in multi-secure network environments, and also the need for continuing industry awareness of network security problems.

Customers or contractors being seriously interested in connecting to governmental network must have all applicable security policies, standards, and procedures, before access is granted. These requirements should ensure that minimum-security practices are always in place. Password protection for local file servers must be enforced for all users before access to the network is granted. Local hosts must report all non-local site accesses. This auditing capability should ensure unauthorised accesses are traceable.

4.4.1 Securing a Network

Add-on controls

Poor administrative practices and the lack of education, tools, and controls combine to leave the average system vulnerable to attack. Research promises to alleviate the inadequate supply of tools and applicable controls. These controls, however, tend to be add-on controls. There is a need for the delivery of secure complete systems, rather than the ability to build one from parts. The average administrator has little inclination to perform these modifications and no idea how to perform them.

Extensive connectivity increases system access for hackers. Until standards become widely used, network security will continue to be handled on a system-by-system basis. The problem can be expected to increase if and when the Integrated Systems Digital Network (ISDN) is implemented without appropriate security capabilities.

A promising note for the future does exist. Multiple sets of tools do not need to be developed in order to solve each of the potential threats to a system. Many of the controls that will stop one type of attack on a system will be beneficial against many other forms of attack. The challenge is to determine what is the minimum set of controls necessary to protect a system with an acceptable degree of assurance.

4.4.1.1 Design of a Secure Network

Ensuring end-to-end security for a secure network

The design of a secure network shall consist of network elements that cater for end-to-end security. The design must first undergo a process of security assessment during which the organisation states its aims and objectives, scope of security and whether there is a need for end-to-end security, inter-network security or security at the internal systems only. From here the organisation then combines the business needs and network risk analysis.

The next step is to identify and determine the assets that need to be protected, including the information types, where and the degree/level of security protection needed. After all assets and their security requirements are determined, the network and systems architecture to support the different objectives and aims has to be established, taking into account the security needs of each system and application.

The design must also identify potential threats and vulnerabilities, and establish the preventive systems, policies and procedures to protect the information. The finished design can take many forms but for the purpose of these guidelines, a generic architecture is described as in the figure below:

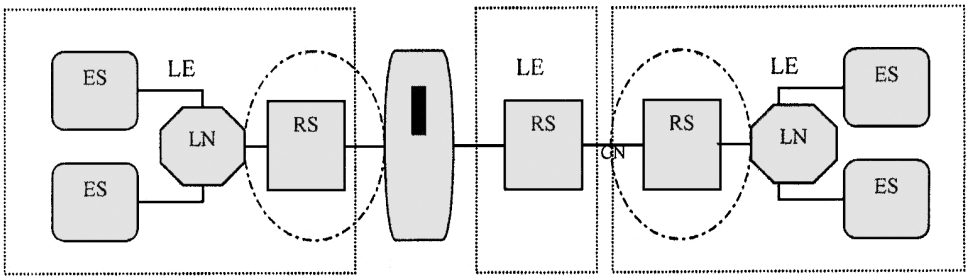

Figure 4.1: Generic Network Security Architecture

Key :

ES = End System	RS = Relay System
LN = Local Network	LE = Local Environment

From Figure 4.1 above, the generic network security architecture applies to any network-to-network connectivity. The most vulnerable part of the network is RS where the router and switches are located. It is at this point of the network that security gateways are normally placed in the form of firewalls or other security equipment that cater for data encryption, data origin authentication, data integrity and access control. All these must also be included based on the requirements identified during the security assessment process.

The security gateways can be a simple firewall that separates connections to other networks and the two network zones; namely the DMZ and the secure zone. It may also include VPN modules and/or encryptors/decryptors.

The other considerations at the department's client premise include the need to have Intrusion Detection System (IDS), virus scanners and data encryption at the local environment (LE). The decision to use IDS is also subject to requirements that are determined during security assessment.

4.4.1.2 Network Security Controls

Ensuring a range of appropriate security controls

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access.

A range of security controls is required in computer networks. Individual users should be aware that connecting their computer to the network could allow unauthorised access to private data if appropriate controls are not established. Documentation should be available to the user detailing how to adequately secure their data should they wish to make it available on a network.

Network managers should ensure that appropriate controls are established to ensure the security of data in networks, and the protection of connected services from unauthorised access. Special attention is required to protect sensitive data passing over public networks like the Internet.

4.4.2 Security of Network Equipment

In order to effectively include security in the procurement process of network systems or equipment, it must be integrated into the procurement cycle from its inception. Sufficient information about the procurement cycle is included to allow a person not familiar with the procurement process to understand the need for incorporating computer security into the procurement cycle.

Acquisition planning can only begin after an agency has determined that a need exists. The need determination phase is very high-level in terms of functionality. No specifics of a system are defined here. The idea for a new or substantially upgraded system and the feasibility of the idea need to be explored. During this early phase of the acquisition, the definition of the security requirement should begin with the preliminary sensitivity assessment.

The preliminary sensitivity assessment should result in a brief qualitative description of the basic security needs of the system. These should be expressed in terms of the need for integrity, availability, and confidentiality. This does not require an elaborate sensitivity analysis scheme, but must include an assessment of the significance of the systems. Legal implications, federal policy, agency policy, and the functional needs of the system help determine the sensitivity of a system. Factors including the importance of the system to the agency mission and the consequences of unauthorised modification, unauthorised disclosure or unavailability of the system or data should be considered when assessing sensitivity.

4.4.2.1 Installation Security

Pre-installation security check

After undergoing a security check during the procurement process, any equipment that is to be installed must have undergone a Factory Acceptance Check (FAC), prior to installation, and then configured.

4.4.2.2 Physical Security

Ensuring physical security

The following standards of physical security must be observed:

(a) premises housing network control equipment must be physically strong and free from unacceptable risk such as flooding, vibration, dust, etc;

(b) air temperature and humidity must be controlled to within equipment defined limits; and

(c) network electronics must be powered via Uninterruptible Power Supply (UPS) to provide the following:

i. minimum of 15 minutes' operation in the event of a power blackout; and

ii. adequate protection from surges and sags.

4.4.2.3 Physical Access

(a) Network Cabling Access

Protection against unauthorised access

As far as practical, network infrastructure must be protected from unauthorised access. Tools are readily available which allow network ports to be monitored, or the operation of the network to be disrupted. In order to minimise the risk of network interference consideration should be given to:

i. protecting cabling in public areas with conduits or other protective mechanisms;

ii. in a structured wiring area, ensure that network and telephone points that are not in use have been detached from the active network or telephony equipment;

iii. telephony and networking risers and data cabinets can only be accessed by authorised personnel;

iv. information, which is being transferred over a less secure network (e.g. the Internet) is encrypted; and

v. highly accessible access points such as networked modems should have associated and appropriate security mechanisms.

(b) Network Equipment Access

All network equipment should be placed in physically secure areas. This includes, but is not limited to, backbone and access routers, hubs, bridges, and gateways. Network file servers are covered by this policy as well, especially when acting as a router between LAN types, such as Ethernet to Token Ring. Networking equipment should not be placed in an office environment. Rather, such equipment should be placed in the communications room of the office building being served, and access restricted to authorised personnel. In addition:

i. access to areas housing network electronics shall be controlled by designated ICTSO; and

ii. doors to areas housing network electronics should be locked with a unique key, the distribution of which will be determined by the ICTSO.

4.4.2.4 Logical Access

(a) An ID and password should be required to gain access to router software. Only authorised personnel should be provided access, along with the minimal privileges required for performing the necessary tasks. The ICTSO administers the creation of the router IDs, passwords and privileges. Proper management authorisation should be required for all access requests. A list of these ‘management authorisers’ must be maintained and updated at least once a year. Requests for access must be maintained for the life of the IDs.

(b) Password composition and maintenance must be consistent with the guidelines. Passwords must be changed approximately every 30 days, as well as after security events, in emergency situations, when an employee transfers, or any other incident in which the password may be compromised.

(c) All access to routers must be logged and maintained, including the person, time of day, and nature of activity. This information must be maintained for 90 days. Daily audit trails are to be monitored for unauthorised access attempts. Managers will take appropriate action with respect to all unauthorised access attempts.

(d) The network should only accept traffic from properly registered addresses. All router software changes must be logged, including the person making the change, management approval of the change, date and time. Access via modem will be accommodated only under strictly controlled conditions.

(e) Router configuration change authority is to be centrally managed. All routers should have active filter tables to ensure that only authorised access is allowed. In environments where information is especially sensitive, additional precautions may be required, such as data encryption, and security gateways. These precautions should be taken as requested or required, and will be offered as additional service to the base level.

4.4.2.5 Unauthorised Use of Equipment

Controlling unauthorised use of equipment

The unauthorised use or interruption of network equipment can be prevented by:

(a) controlling access to network equipment by logical access controls listed above;

(b) locating network equipment in a physically secure environment;

(c) erecting a physically secure wiring closet, accessible only by authorised personnel;

(d) routing network cabling underground or through conduits, wherever possible;

(e) maintaining an inventory of network equipment, which is periodically reviewed; and

(f) prohibiting the use of any unauthorised modem.

4.4.2.6 Equipment Configuration

Ensure correct configuration of equipment

On critical network subnets, it is absolutely important to correctly configure network equipment. It is imperative to check for the following:

(a) enable only needed services;

(b) restrict access to configuration services by port/interface/IP address;

(c) disable broadcasts;

(d) choose strong (non default) passwords;

(e) enable activity logging; and

(f) carefully decide who should have user/enable/administration access.

4.4.2.7 Equipment Maintenance

Proper maintenance of equipment

Equipment should be installed, operated and maintained according to the manufacturer's specifications. Properly qualified personnel should carry out maintenance.

Equipment should:

(a) be installed and operated within the manufacturer's specifications;

(b) be maintained in accordance with the manufacturer's recommended service intervals and specifications;

(c) be repaired and serviced only by properly trained and authorised service personnel; and

(d) have a maintenance record of all faults or suspected faults. Not only does this aid the diagnosis and repair procedure, but may be used to document warranty and other claims.

Ensure that the integrity of security controls is maintained during equipment maintenance by:

(a) allowing modifications to be made only by authorised personnel within established maintenance procedures;

(b) insisting on testing of controls, both before and after maintenance changes;

(c) maintaining a record of all faults or suspected faults;

(d) ensuring virus checks are made where appropriate; and

(e) tamper-protecting components which store sensitive information.

4.4.2.8 Disposal of Equipment

Proper disposal of equipment to prevent disclosure of sensitive information

In order to prevent disclosure of sensitive information through disposal of equipment conduct the following:

(a) check all equipment containing storage media for sensitive information prior to disposal;

(b) perform a risk assessment on damaged equipment to determine if it should be destroyed, repaired or discarded; and

(c) ensure storage media undergo a secure erasure procedure prior to disposal.

4.4.3 Securing Different Modes of Communications

Security threats from different modes of communications

Different modes of communications discussed in this section include wired and fixed network, wireless communications, microwave communications and satellite. These different modes pose different types of security threats and ways of prevention as discussed below.

4.4.3.1 Wired Network

A wired Network is a network that uses the conventional copper or more recently, the optical fibre as the medium of communication. Presently, the wired network is the most predominant in the networking world as can be seen in the next paragraph.

Apart from the telephone private networks, one of the fastest growing sector is the area of Local Area Network (LAN). An area that is growing at an even faster rate is the product that links multiple LANs together. Hence, today the Internet is seen as an explosion of networks inter-linking thousands and millions of LANs. Today these networks are interconnected through physical wires or cables, especially LANs. However, the availability of wireless LANs will certainly change the future network environment.

4.4.3.2 Wireless Communication

Wireless applications involve the technology of presenting and delivering wireless communication information to and from telephony terminals, other wireless terminals, within a LAN and within networks. A wireless application is utilised when a telephony terminal, e.g. mobile phone communicates with a server installed in the mobile telephony network.

Wireless LAN systems are usually made up of a cell or group of cells that contain several wireless station adapters in each of them. Each cell is controlled by an Access Point, (a device that is usually connected to an existing backbone), and which manages all the traffic within the cell. Station adapters within the coverage area of an access point (i.e. the cell) can communicate between themselves, or gain access to wired LAN resources through the access point. Station adapters associated with an access point are synchronised with it by both frequency and clock, so they can transmit and receive data to and from the access point. The same rule applies for interception - in order for someone to intercept the data one must be within the coverage area of the cell and be synchronised with the access point.

There are two types of wireless protocols that are widely used today. Direct Sequence (and also narrow band) wireless LAN systems work in a predefined constant frequency, i.e. when the user buys an access point or a station adapter it is working in a certain constant frequency. In this case it is easier to detect the frequency of the carrier wave and to synchronise with it. With Frequency Hopping systems, the frequency of the carrier wave is continuously changing. It is difficult to detect the current frequency of transmission and even if it is possible, it changes within milliseconds.

Secure wireless connection can be assured by:

(a) implementing a secure wireless protocol that will uphold data integrity, privacy, authentication and protect from denial-of-service;

(b) providing controls for the detection and reporting of dropped communications and timely termination of all associated sessions; and

(c) requiring re-authentication when wireless connection drops occur.

Eavesdropping of the wireless signalling can be prevented by:

(a) establishing a policy setting out conditions under which wireless access is permissible;

(b) implementing, where business needs dictate, additional controls such as, frequency hopping;

(c) encrypting classified information during electronic transmission; and

(d) protecting passwords by encryption.

Corruption or modification of information during transmission can be detected by authenticating information with digital signature. Establishing a procedure for safeguarding and use of wireless equipment can prevent unauthorised use or interruption of wireless equipment such as wireless network access equipment, wireless PC cards and Wireless Applications Protocol (WAP) enabled devices.

4.4.3.3 Microwave Communication

Some parts of the government network will include microwave communications systems as part of the overall infrastructure. Microwave equipment uses 'focused' transmission techniques between transmitting and receiving dishes. Microwave communication is basically a Frequency Modulation (FM) radio at a specific frequency and modulation. It is a point-to-point of line-of-sight communications.

A security procedure should be established to ensure secure microwave communications as follows:

(a) data encryption - a clear procedure on data/information transmission;

(b) physical access - access to communications equipment (network facilities) should be controlled and restricted;

(c) provide controls for monitoring, detecting and reporting of dropped communications due to Radio Frequency Interference (RFI), weather effects, etc; and

(d) provide control over acquisition processes by ensuring appropriate equipment is purchased.

4.4.3.4 Satellite

The primary role of a satellite is to reflect electronic signals. In the case of a telecom satellite, its primary task is to receive signals from one ground station and send them down to another ground station located a considerable distance away from the first. This relay action can be two-way, as in the case of a long distance phone call.

Another use of the satellite is when, as is the case with television broadcasts, the ground station's uplink is then downlinked over a wide region, so that it may be received by many different customers possessing compatible equipment. Still another use for satellites is observation, wherein the satellite is equipped with cameras or various sensors, and it merely downlinks any information it picks up from its vantage point.

The advantage of satellite communications is a high degree of reliability and availability. Furthermore, satellite operator normally add back-up satellites to further enhance the already high degree of redundancy. There is also very minimum number of points where network security vulnerabilities exist (i.e. the satellite itself and the ground station). However, satellite communications normally co-exist with fixed network communications. This requires security measures and procedures to be applied according to the fixed network guidelines.

4.4.4 User Accessibility

Assigning user accessibility

As a general rule, the assignment of network access privileges and control of proxy accounts and default network accounts for all network users shall be centrally controlled, authorised and documented.

The material presented below may be used to formulate a policy on network services.

4.4.4.1 Local Area Network

Within the boundaries of the LAN, intrusion protection is required to prevent:

(a) government employees from indiscriminately plugging laptop computers into any access port of the LAN;

(b) unauthorised access of government employees to strategic systems, by ensuring that:

i. only those computers belonging to the Government will be allowed to function when connected to the LAN. Visiting personnel wishing to access the network must have authorisation from the system administrator, who must apply to the ICTSO for temporary access rights; and

ii. no unauthorised user should be allowed network access to strategic computing systems.

Insider attacks or unauthorised access to internal networks can be prevented by the following measures (note: most attacks come from the inside):

(a) no 'sniffer' or 'network analyser' software is to be allowed on any PC unless it has been authorised by the network manager in consultation with the ICTSO. The status of these machines should be reviewed yearly;

(b) on systems, where such software utility is standard, the software should either be deleted or permissions changed so that it can only be used by root. In this case the user must not have access to the root account; and

(c) installing a packet filter/firewall between internal networks and class systems.

Hubs, bridges and routers are getting very intelligent, with more and more configuration options and are increasingly complex. This is useful for additional features, but the added complexities increase the security risk.

4.4.4.2 Remote Access

Remote access is the capability to access information-processing resources via public or private networks. In order to ensure that remote access controls are not compromised the following need to be adhered to:

(a) establish a policy stating the conditions where remote access is permissible;

(b) implement additional controls (according to business needs) such as token-based authentication devices, security modems that can provide password and dial-back controls or remote computing software that can provide password controls;

(c) require written permission when external access is absolutely necessary. These external connections can be classified as incoming or outgoing; and

(d) use secure remote access approved equipment.

Examples of incoming connections are:

(a) dial-up access for organisation / partners;

(b) dial-up access for ICT staff and directors;

(c) access from universities (co-ordination on research projects);

(d) Internet e-mail;

(e) enterprise WWW server; and

(f) Electronic Data Interchange (EDI).

Examples of outgoing connections are:

(a) access to vendor bulletin boards (for getting information, drivers);

(b) customer connections (providing special services to public);

(c) Internet e-mail;

(d) normal Internet access: WWW e.g. Netscape/Internet Explorer via proxy server;

(e) special Internet access: e.g. Archie, ftp, news, telnet, gopher and WAIS; and

(f) EDI.

External contractors must also comply with the public sector's ICT Security Policy. In addition, the department needs to:

(a) execute a written agreement with external parties identifying security roles and responsibilities;

(b) establish a procedure requiring the intervention of an authorised employee to enable/disable a remote access session; and

(c) review activity logs of each remote access session.

4.4.4.3 Dial-up Access

Systems accessible from dial-up terminals are particularly vulnerable to unauthorised access since the call can be initiated from virtually any telephone instrument. Official users of dial-up facilities must be distinguishable from public users if they are to be given access rights greater than those given to public users.

For services other than those authorised for the public, users of dial-up terminals shall be positively and uniquely identified and their identity authenticated (e.g., by password) to the systems being accessed.

For dial-up services other than those authorised for public use, the following should be considered:

(a) dial-up numbers should be unlisted and changed periodically;

(b) at a minimum, dial-up facilities should be provided with either:

i. an automatic hang-up and call-back feature, with call-back to only pre-authorised numbers; or

ii. authentication systems that employ smart card/token authentication.

(c) a port protection device (PPD) connected to communications ports of a host computer is typically capable of providing:

i. authentication and access control decisions;

ii. automatic hang-up and call-back to originator; and

iii. attack signalling and event logging.

(d) security may be enhanced by instituting a two-person password procedure. One person's password gains access to the host and the other person's password gains access to the application. Under this procedure, neither acting alone can gain access to the application through dial-up; and

(e) a high level of dial-up security combines the call-back feature with either password authentication (an encryption key entered by the individual or smart card/token authentication) and terminal identification (an encryption key embedded in the hardware), with all data exchanged on-line being encrypted.

For dial-up facilities authorised for public use, take into consideration the following:

(a) systems which allow public access to the host computer require strengthened security at the operating system and applications level to reduce the likelihood of public intrusion into non-public applications. Such systems also should have the capability to monitor activity levels;

(b) ensure public usage does not unacceptably degrade system responsiveness for official functions; and

(c) systems which identify public users on the basis of communications port usage provide only minimal security since they are highly vulnerable to mistakes through erroneous hardware connections.

4.4.4.4 Virtual Private Networks

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and other security procedures. A VPN is similar to a system of owned or leased lines that can only be used by an organisation.

The idea of the VPN is motivated by the need for secure communication between computer networks in different locations with the same capabilities at much lower cost by using shared public infrastructure rather than a private one. This is especially important for government agencies that need connectivity between geographically distributed branch offices.

VPNs allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. Since some firewalls provide VPN capability, it is necessary to define the policy for establishing VPNs.

Any connection between firewalls over public networks shall use encrypted VPNs to ensure the privacy and integrity of the data passing over the public network. All VPN connections must be approved and managed by the System Administrator. Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

Due to sharing of resources, a government agency that wishes to employ a VPN should have the following:

(a) a firewall located at a network gateway that protects the resources of a private network from users of other networks. Firewalls are implemented at the session layer of the network. This is to filter access and block unwanted users from the system. Therefore, government agencies should have defined policies, where change of policies are driven by the changing security requirements of those agencies;

(b) a firewall is installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources;

(c) allow to securely connect branch offices, telecommuters, mobile users, and selected parties to be securely connected to data resources by taking advantage of the cost effectiveness of the Internet; and

(d) remote users be given controlled access to selected servers (enforced path) and applications on the network or DMZ.

4.4.5 Connection with other Networks

With regard to other network connections some of the following should be undertaken to ensure ICT security is maintained:

(a) obtain specific authorisation from the ICTSO for connection to networks not under the organisation's control;

(b) establish written policies and procedures for connection to external networks; and

(c) impose on the security policy of the external provider requiring it to be verifiably as strong as the organisation's own network security policy.

Outside penetration or unauthorised access of the network can be prevented by:

(a) using fibre optics for internal cabling rather than the UTP cables because they are very difficult to interrupt or sniff (especially for very secure environment);

(b) minimising the installation of network protocols e.g. do not install NetBEUI on sub-netted networks, use TCP/IP & WINS servers instead;

(c) avoiding the use of Workgroups (i.e. disable workgroups). This is because workgroups support share-level security, but not user-level security. Organisations are advised to use Domains (LAN-Manager, NT) or NFS instead; and

(d) disabling floppy boot in PC client's BIOS set-up. Furthermore, PC clients should not be used as ftp or http servers.

4.4.5.1 Integrity of Connections

The capture of a session during accidental or intentional communication line drops can be prevented by:

(a) providing network controls for the detection and reporting of dropped communications lines and timely termination of all associated computer sessions; and

(b) adding a procedure that requires re-authentication when line drops occur.

4.4.5.2 Firewalls

The increased use of the Internet has made computer technology more useful but on the other hand, has resulted in the networking environment becoming more dangerous. This is because the Internet now also presents unprecedented opportunity for attack. Any computer user can subscribe to an Internet Service Provider (ISP) and become a true network 'node'. As a result there is no control over who can be on the Internet or what they use it for.

There is a dire need to protect systems on the Internet from both known and unknown assaults from a vast pool of attackers. What can generally be used to protect users from outside attacks can take the form of a firewall.

A firewall can be defined as a collection of components deployed between two networks that collectively have the following properties:

(a) all traffic from inside to outside, and vice-versa, must pass through the firewall; and

(b) only authorised traffic will be allowed to pass, as defined by the local ICT security policy.

A well-designed firewall is able to protect an organisation's network and ICT resources as well as those communicating partners' networks interconnected through the same firewall. Attacks from within the institution's network, or that of its communicating partner, must be addressed by using other security facilities.

Firewalls specified for use in a secure governmental institution should be designed for the following considerations:

(a) strong authentication and identification;

(b) a high degree of confidence of knowing who an institution is dealing with. A secure identification of the communication partner must precede any authorisation to conduct business. The ability of identifying who is using a system is required to prevent unauthorised use and to aid investigation of attacks;

(c) audit and archive requirements;

(d) the activity through a firewall contains information, which must be archived for a certain time to provide evidence, if necessary. Auditable security-related events also must be properly captured;

(e) availability;

(f) only reliable services should be provided;

(g) confidentiality; and

(h) confidence that governmental information will remain mandatorily protected.

Suggestions for proper selection and implementation of firewall

Due to the fact that the Internet environment is constantly changing, it is difficult to specify exhaustively all the requirements for firewalls. However, the following suggestions, where applicable, should form the basis of proper firewall selection and implementation:

(a) Technical Design Axioms

i. All connections to the institution's networks must be properly controlled;

ii. No IP packets will be exchanged between networks and the Internet except through the connection established through the firewall; and

iii. Traffic is exchanged through the firewall at the application layer only. Institution's hosts,which support incoming service requests from the public through the Internet will sit outside the firewall.

(b) Firewall Attributes	i	The firewall systems will be implemented to work within the constraints of internal network routing technical features;
	ii.	The firewall must enforce a protocol discontinuity at the transport layer;
	iii.	The firewall must not switch any IP packets between the protected and unprotected networks;
	iv.	The firewall must hide the structure of the protected network;
	v.	The firewall must provide an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected;
	vi.	The firewall system must use a 'proxy server' to provide application gateway function through the firewall;
	vii.	Routes through the firewall must be statically defined and the firewall configuration protected;
	viii.	The firewall must not accept session initiation from the public Internet;
	ix.	The firewall system must defend itself from direct attack;
	x.	The firewall must be structured so that there is no way to bypass any firewall component; and
	xi.	The firewall must include an application 'launch server' to support application connections from user systems to Internet services.
(c) Proxy Server Attributes	i.	The proxy server acts as an application gateway;
	ii.	The proxy server hides internal details of the protected network from the public Internet;
	iii.	The proxy server does not switch any network level packets;
	iv.	The proxy server logs all activity in which it is involved; and
	v.	There are no user accounts on the proxy server itself.
(d) Launch Server Attributes (Web Based Application Server)	i.	The launch server houses only client applications;
	ii.	User logins on the launch server must be different from the user's 'home account'; and

iii. Where possible, the launch server should be based on a hardware and software platform different from the user's home systems.

4.4.5.3 Public Users

Where public users are authorised access to networks or host systems, these public users as a class must be clearly identifiable and restricted to only services approved for public functions. Employees who have not been assigned a user identification code and means of authenticating their identity to the system are not distinguishable from public users and should not be afforded broader access.

4.4.5.4 Distributed Network Access

Owners of distributed information resources served by distributed networks shall prescribe sufficient controls to ensure that access to those resources is restricted to authorised users and uses only. These controls shall selectively limit services based on:

(a) user identification and authentication (e.g., password, smart card/ token);

(b) designation of other users, including the public where authorised, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session; or

(c) physical access controls.

In a distributed network access to distributed processing systems and LAN, the following are recommended:

(a) authorisation at network entry should be made on the basis of valid user identification code and authentication (e.g., password, smart card/token) and should be provided under the framework of network services and controlled by the network management programme;

(b) network access should be controlled as close to the physical point of network entry as possible;

(c) connections between users on a network should be authorised by the host or the network node security manager programme, as appropriate;

(d) the designated manager of an independent network host serves the dual role as owner of the network system and as custodian of data under another's ownership while the data is being transported by the network;

(e) the host security management programme should maintain current user application activity authorisations through which each request must pass before a connection is made or a session is initiated;

(f) all unauthorised attempts (successful or otherwise) to access or modify data through a communication network should be promptly investigated; and

(g) if unauthorised access or modification of data occurs, the agency should promptly review its existing security system, including its internal policies and procedures. Appropriate corrective actions should be planned for and established to minimise or eliminate the possibility of recurrence. Employees may also need to be reminded of existing or revised procedures.

Government departments provide services to the public. In many cases members of the public require access to public sector ICT systems. In order to protect against unauthorised access from external users, the public domain information should be held separate (if possible) from corporate information. All access from external users is required to be routed through the department's firewall.

4.4.6 Protection during Transmission

Classified information must be prevented from disclosure during transmission by:

(a) encrypting classified information during electronic transmission; and

(b) protecting passwords by encryption during transmission, where possible.

Classified information must be protected from being corrupted or modified during transmission by authenticating information through approved digital signature.

4.4.6.1 Uploading & Downloading within Intranet

Uploading and downloading allow users to receive and send electronic files in a point-to-point manner. This service is developed to ease exchanging of document between two parties via electronic file transfer. It can create, replace, delete or copy document from one another.

Controls that should be implemented to protect uploading and downloading are as follows:

(a) Authorised User

Only authorised users are to perform uploading or downloading and this can be assured by restricting access to this service capability by logical access control;

(b) Physical Protection

The following can prevent destruction of information and information processing capability through access of equipment providing uploading and downloading services:

i. restricting physical access to information processing resources supplying uploading and downloading services;

ii. uploading and downloading services should reside in their own host;

iii. the service offered for external use should not be hosted in the same server or co-located with services offered for internal use; and

iv. uploading and downloading services for external use with weak or no security features should be prohibited.

4.4.6.2 Uploading & Downloading to/from the Internet

Uploading and downloading to/from the Internet is aimed at providing the capability to search for information related to business needs. Individuals and groups with such functions will be provided with Internet access capabilities.

4.4.7 Network Monitoring

Preventing exploitation of network vulnerabilities

Network vulnerabilities are those that can be exploited, whenever a system has the capability to electronically send information to or receive information from another system.

These vulnerabilities exist primarily in two areas:

(a) interception of information during transmission; and

(b) non-detection of improper messages and message headers received by the system.

Whenever the system is used to electronically send information to or receive information from another computer system, there is a chance that the information will be intercepted while en route. Therefore, steps should be taken to ensure that no information is compromised during transmission.

4.4.7.1 Problems to be Monitored

ICT based systems face new challenges not found under paper-based environment. Information been digital in nature is susceptible to a series of vulnerabilities such as:

(a) Trojan Horse and covert channel

i. Vulnerabilities

- disgruntled valid users;
- computer equipment is located in open areas;
- client stations are not password protected at boot time; when users are away from their computers, they tend to leave them still logged in to the network; and
- highly vulnerable network.

ii. Safeguards

- minimum reliability checks done on all employees;
- auditing of access to data;
- access to user accounts limited by client stations address (Novell feature); and
- ACLs are set in such a way that all the executables stored on the network can only be executed, i.e. they cannot be copied, deleted or modified.

(b) Eavesdropping

i. Vulnerabilities

- connections made with unshielded twisted-pair cables;
- no tempest or low emanation equipment used;
- monitors located beside windows;
- printers located in open areas and close to windows; and
- Ethernet topologies are used (data is broadcasted on network segments); and

ii. Safeguards

- physical access control; and
- fibre optics used.

(c) Virus on the Network

i. Vulnerabilities

- no virus scan or virus detection tool implemented;
- numerous uncontrolled external network connections via client stations;
- network start-up files are stored on each client stations; and
- placement of monitors/printers.

ii. Safeguards

- installation of virus scanning tools;
- access control features, which provide protection against unauthorised access to the network;
- weekly back-ups;
- security procedures such as stating that floppy diskettes external to the network should not be used on client stations; and
- encryption

(d) Intruders

Insiders and hackers are the main components of the human threat factor. Insiders are legitimate users of a system. When they use their access rights to circumvent security, this is known as an insider attack. Hackers, the most widely known human threat, are people who enjoy the challenge of breaking into systems.

(e) Insider Attacks

The primary threat to computer systems has traditionally been the insider attack. Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Insiders can plant Trojan Horses or browse through the file system. This type of attack can be extremely difficult to detect or protect against.

The insider attack can affect all components of computer security. Browsing attacks the confidentiality of information on the system. Insiders can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

These attacks are possible for a variety of reasons. On many systems, the access control settings for security-relevant objects do not reflect the organisation's security policy. This allows the insider to browse through sensitive data or plant Trojan Horses. The insider exploits operating system by planting bugs to cause amongst others the system to crash.

The actions are undetected because audit trails are inadequate or ignored.

(f) Hackers

The definition of the term 'hacker' has changed over the years. A hacker was once thought of as any individual who enjoyed getting

the most out of the system he was using. A hacker would use a system extensively and study the system until he became proficient in all its nuances. This individual was respected as a source of information for local computer users; someone referred to as a 'guru' or 'wizard'. Now, however, the term hacker is used to refer to people who either break into systems for which they have no authorisation or intentionally overstep their bounds on systems for which they do not have legitimate access.

Methods used by hackers to gain unauthorised access to systems include:

i. password cracking;

ii. exploiting known security weaknesses;

iii. network spoofing; and

iv. 'social engineering'.

The most common techniques used to gain unauthorised system access involve password cracking and the exploitation of known security weaknesses. Password cracking is a technique used to surreptitiously gain system access by using another user's account. Users often select weak passwords. The two major sources of weaknesses in passwords are easily guessed passwords based on knowledge of the user (e.g. wife's maiden name) and passwords that are susceptible to dictionary attacks (i.e. brute-force guessing of passwords using a dictionary as the source of guesses).

Another method used to gain unauthorised system access is the exploitation of known security weaknesses. Two types of security weaknesses exist: configuration errors, and security bugs. There continues to be an increasing concern over configuration errors. Configuration errors occur when a system is set up in such a way that unwanted exposure is allowed. Then, according to the configuration, the system is at risk from even legitimate actions. An example of this would be that if a system 'exports' a file system to the world (makes the contents of a file system available to all other systems on the network), then any other machine can have full access to that file system (one major vendor ships systems with this configuration).

Security bugs occur when unexpected actions are allowed on the system due to a loophole in some application programme. An example would be sending a very long string of keystrokes to a screen-locking programme, thus causing the programme to crash and leaving the system inaccessible.

A third method of gaining unauthorised access is network spoofing. In network spoofing a system presents itself to the network as though it were a different system (system A impersonates system B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other 'trusted' systems. Trust is imparted in a one-to-one fashion; system A trusts system B (this does not imply that system B trusts system A). Implied with this trust, is that the system administrator of the trusted system is performing his job properly and maintaining an appropriate level of security for his system. Network spoofing occurs in the following manner: if system A trusts system B and system C spoofs (impersonates) system B, then system C can gain otherwise denied access to system A.

'Social engineering' is the final method of gaining unauthorised system access. People have been known to call a system operator, pretending to be some authoritative figure and demanding that a password be changed to allow them access. One could also say that using personal data to guess a user's password is social engineering.

4.4.7.2 How to Overcome Insider Attacks and Hackers

Today, desktop workstations are becoming the tool of more and more scientists and professionals. Without proper time and training to administer these systems, vulnerability to both internal and external attacks will increase. Workstations are usually administered by individuals whose primary job description is not the administration of the workstation. The workstation is merely a tool to assist in the performance of the actual job tasks. As a result, if the workstation is up and running, the individual is satisfied.

This neglectful and permissive attitude toward computer security can be very dangerous and has resulted in poor usage of controls and selection of easily guessed passwords. As these users become, in effect, workstation administrators, this problem will be compounded by configuration errors and a lax attitude towards security bugfixes. In order to correct this, systems should be designed so that security is the default and personnel should be equipped with adequate tools to verify that their systems are secure.

Of course, even with proper training and adequate tools threats will remain. New security bugs and attack mechanisms will be employed. Proper channels do not currently exist in most organisations for the dissemination of security related information. If organisations do not place a high enough priority on computer security, the average system will continue to be at risk from external threats.

System controls may not matched well to the average organisation's security policy. As a direct result, the typical user is permitted to circumvent that policy on a frequent basis. The administrator is unable to enforce the policy because of the weak access controls, and cannot detect the violation of policy because of weak audit mechanisms. Even if the audit mechanisms are in place, the daunting volume of data produced makes it unlikely that the administrator will detect policy violations.

On-going research in integrity and intrusion detection promises to fill some of these gaps. Until these research projects become available as products, systems will remain vulnerable to internal threats.

Connectivity allows the hacker unlimited and virtually untraceable access to computer systems. Registering a network host is akin to listing the system's modem phone numbers in the telephone directory. No one should do that without securing his or her modem lines (with dial-back modems or encryption units). Yet, most network hosts take no special security precautions for network access. They do not attempt to detect spoofing of systems; they do not limit the hosts that may access specific services.

A number of partial solutions to network security problems do exist. Examples include Kerberos, Secure NFS, RFC 931 authentication tools and 'tcp wrapper' programmes (access controls for network services with host granularity). However, these tools are not widely used because they are partial solutions or because they severely reduce functionality.

New solutions for organisations are becoming available, such as the Distributed Intrusion Detection System (DIDS) or filtering network gateways. DIDS monitors activities on a subnet. The filtering gateways are designed to enforce an organisation's network policy at the interface to the outside network. Such solutions may allow the organisation to enjoy most (if not all) of the benefits of network access and at the same time limit the hackers' access.

4.4.7.3 Monitoring Tools

Information disclosure, modification, or destruction by use of monitoring devices can be protected by:

(a) implementing use and storage controls over devices that monitor or record information being transmitted on a network (e.g., protocol analysers and Intrusion Detection System). The use of this equipment must have the consent of the ICTSO;

(b) ensuring that employees understand, as part of their condition of employment, that use of the organisation's information processing assets constitutes consent to monitoring; and

(c) continuing quality of controls must be ensured by maintaining an audit trail.

Many intrusion detection systems (IDS) base their operations on analysis of OS audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

An IDS may also perform its own system monitoring. It may keep aggregate statistics, which give a system usage profile. These statistics can be derived from a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the state of the current system state. They are correlated with an internal model which will allow the IDS to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system.

An intrusion detection system should address the following issues, regardless of what mechanism it is based on:

(a) it must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a 'black box'. That is, its internal workings should be examinable from outside;

(b) it must be fault tolerant in the sense that it must survive a system crash and not have its knowledge base rebuilt at restart;

(c) on a similar note to the above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted;

(d) it must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used;

(e) it must observe deviations from normal behaviour;

(f) it must be easily tailored to the system in question. Every system has a different usage pattern, and the defence mechanism should adapt easily to these patterns;

(g) it must cope with changing system behaviour over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt; and

(h) finally, it must be difficult to fool.

4.5 Security Posture Assessment of ICT

Security management is an on-going process

At anytime, the management of an organisation must be aware of the true level of its entire ICT security. This is because the security of a system is only as strong as its weakest point. No organisation should feel complacent about its state of security. There are continuously discovered vulnerabilities and bugs in operating system services, application software components, web browsers and e-mail systems.

What is a security posture assessment

The security state (posture) of an organisation must be assessed and a baseline established for continuous improvement. In the assessment process, existing policies (if any) and their implementation will be reviewed, installation validated and all points of entry into the network checked. Securing a system requires a proper set-up of all devices and services as well as the use of appropriate security tools. This is to minimise the risk of exposure to attacks through a non-technical approach such as social engineering that may defeat any technical means.

The security posture assessment (SPA) is performed to establish the current baseline security of the network and systems by discovering known vulnerabilities and weaknesses, with the intention of providing incremental improvements to tighten the security of the network and systems. The entire process can be divided into three (3) stages:

Stage 1: System/Network Architecture and Policy Review

Stage 2: System Testing and Network Penetration

Stage 3: Report/recommendation

Planning for a security posture assessment

Unless an organisation has the expertise and tools, an SPA exercise in the public sector could be outsourced to an independent 3rd party. The appointment of the consultant will conform to existing government procedures (*Pekeliling Perbendaharaan 3/95*). Care has to be taken since some information is highly sensitive and usually there are legal implications to be considered (for example the Official Secret Act 1972). An SPA starts with a rigorous and proper plan and this includes:

(a) obtaining the commitment of the management to allocate resources, e.g. documents about system architecture, network topology, application systems installed;

(b) requesting sufficient fund if the SPA is to be outsourced to an outside party;

(c) identifying contact persons in the organisation;

(d) establishing a communication plan during the SPA;

(e) establishing scope of the SPA (i.e. which computers, network devices and application systems will be included);

(f) scheduling the activity to minimise disruption of normal activity; and

(g) eventually detailing the day-to-day activities of the SPA exercise.

Finally, following submission of the SPA report, an organisation will seek to implement recommendations to improve its security level.

Note: The implementation stage is not part of the SPA exercise.