New Zealand Security of Information Technology Publication 100

THE SECURITY OF COMPUTER SYSTEMS

CHAPTER 1

THE VULNERABILITIES OF COMPUTER SYSTEMS

Introduction

101. One of the purposes of the Official Information Act 1982 is to ensure that official information is protected to the extent consistent with the public interest. While all departments should take specific steps to ensure the privacy of personal information, in some cases further protection of information is required as a result of specific legislation relating to the department. Security requirements affect all forms of information, whether on paper or held in electronic or magnetic form on computer memories, communications lines, computer disks and tapes, or computer screens.

102. Computer based information needs to be protected from unauthorised modification or removal, and departments need to ensure that their systems provide information which is accurate, reliable, and available to authorised users in a timely manner. The protection of information processed by computer systems is known as computer security and covers the three properties of information confidentiality, availability and integrity.

103. The advent of microcomputers and the increasing power of low cost multi-user systems has provided departments with highly efficient and accessible data storage and processing facilities; but these systems also expose departments to a higher risk of accidents and deliberate attack. The major aspects of concern are:

a. **Density of Information**. Computer systems can provide rapid analysis of extremely large amounts of raw data to produce refined information, potentially of a higher value, sensitivity or classification than the individual data items. Data communication systems allow large volumes of data to be rapidly and covertly copied to remote computers for later detailed analysis or disclosure.

b. **System Accessibility**. Computer systems are often designed to provide the maximum computing support to the largest possible user community. Many control mechanisms were designed for batch oriented computers located within a physically secured computer centre, but systems are now often widely distributed and located in normal office working environments.

c. **Complexity**. Modern computer systems contain very large numbers of hardware circuits and software instructions, and this complexity makes hardware or software tamper detection very difficult.

d. **Electronic Vulnerability**. Computer systems are vulnerable to electronic attacks because of the technology used to process and store information.

104. Many external factors affect the risk levels to which computer systems are exposed, and as external factors change so different protection is required to maintain a consistent level of security. It is important to ensure that security planning takes into account more than just immediate risks because the external environment can often change faster than new protection measures can be retrofitted.

The Environment, Accidents, and Personnel

105. Traditionally, accidents and negligence have been the major culprits in the loss of availability or integrity in computer systems. The environment is a source of potential disasters such as fire, flood, earthquake, and power failure, and negligence in the development, operation, maintenance and use of computer systems can cause information corruption or system failure. Loss of key personnel through accident or resignation can lead to problems which indirectly affect security. Contingency plans and backup procedures are commonly used to protect against these risks.

Computer Security Model

106. It is useful to think in terms of a framework within which the various components of computer security can be related. The model used in this document is shown in the following diagram:

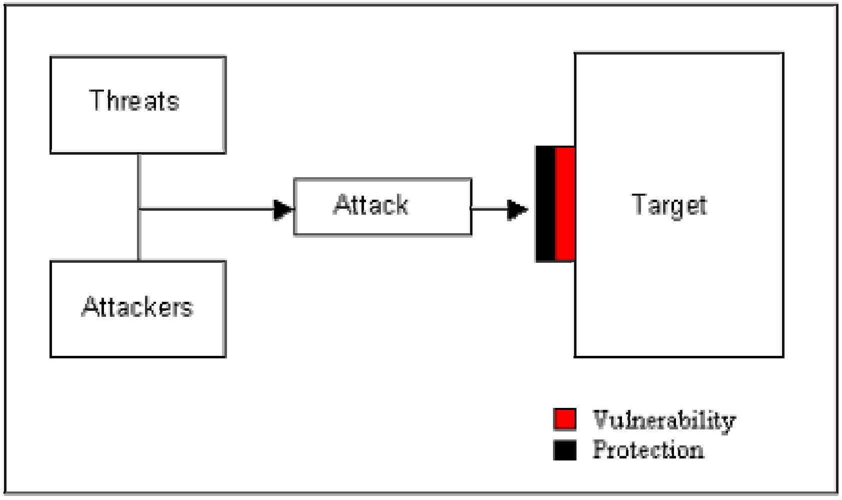

Figure 1: Model of Computer Security

Threats

107. **Sabotage**. Sabotage is the generic name given to the class of deliberate and directed attacks which damage or destroy assets. A sabotage attack can be a physical attack on the facilities, communications lines, or computer equipment, or an electronic attack on software or data. While the normal virus attack is indiscriminate and therefore classed as vandalism, a virus written to attack a particular site or software product would constitute an electronic sabotage attack. Logic Bombs are a particularly significant sabotage threat whereby disgruntled computer staff put hostile program code into a computer system to be triggered at some later and generally predetermined time.

108. **Fraud**. Computer fraud is an attractive form of criminal activity, and is most prevalent in financial systems. Computer fraud is the class of attack which misuses a computer system to obtain a fraudulent pecuniary advantage; it is not an attack on the computer system itself. There are four common and distinctive attacks: deception, salami attacks, ghost employees, and phoney claims. *Deception* , or masquerade, occurs when an attacker identifies himself or herself as an authorised recipient, and obtains money that rightfully should be provided to someone else. *Salami attacks* are those that take a small amount of money from many accounts, typically during such operations as interest calculations. *Phoney claims* are fraudulent claims raised and authorised by an authorising officer. *Ghost Employees* are fictional employees created for the purpose of fraudulently obtaining payroll funds.

109. **Theft**. Theft involves taking items with an intention to permanently deprive their owner of possession. Portable microcomputers are particularly at risk due to the ease with which they can be removed. Internal components of a computer system, such as hard disks and add-on boards, are also easy to remove and their absence will be detected only when the system is next used.

110. **Vandalism**. One of the most popular contemporary types of computer attack is vandalism, carried out through the use of virus and trojan horse programs. Such programs may be relatively benign with the attack phase doing nothing more than playing a tune, or they may be quite malevolent and, for example, reformat the hard disk. Viruses are not directed and will attack any host they happen to infect. Virus attacks are particularly insidious; while dormant they spread covertly throughout many computer systems before beginning their attack cycle. With large numbers of microcomputers being used in departments for day to day activities, and as departments move more into open architecture technology, the risk of infection increases substantially.

111. **Interception**. Interception of automated information occurs primarily in four ways: overview, communications interception, interception of electromagnetic radiation (EMR), and data interception within a computer system.

a. **Overview**. Overview involves gaining visual access to information, typically from some distance away. Hard copy documents and computer screens located near windows are vulnerable to overview.

b. **Communications**. Communications lines connecting independent computer systems are vulnerable to interception by line tapping, by close proximity induction, or, in the case of fibre optic, by a form of refraction known as cohesive detection. Radio frequency and cellular communications are particularly vulnerable to interception. Of particular concern in data communications is the common practice of sending user identification codes (userid) and passwords from remote terminals to their host computers without using any form of data encryption. If this information is intercepted then access control to the host will be totally compromised. This vulnerability is particularly significant if public networks are used as the communications path.

c. **EMR**. Commercial computer equipment generally conforms to national standards for limiting radio frequency interference, but the equipment still emits significant radiation over a wide range of frequencies. In many cases the emitted radiation can be detected at quite significant distances and can be interpreted to reveal the source information. Major sources of compromising emanations include video screens, video screen cables, communications ports, and keyboards. A related problem is the inadvertent induction of information into associated power cables. Equipment to carry out a limited EMR attack is readily available at relatively low cost from electronic hobby stores.

d. **Computer Information**. Information can be intercepted, damaged, or destroyed while being processed within a computer system. Infiltration and interception programs can be written for any computer system, and consist of three major functions or phases:

(i) infiltrating the computer in some way - logic bombs and viruses are examples of this;

(ii) intercepting or corrupting information being processed; and

(iii) if required, extracting the intercepted information.

112. **Misuse**. Misuse of software and data is the unauthorised access to, use, or copying of software or data. This can be done remotely if systems allow outside electronic access through dial-in or network connections. The simplest form of misuse is copying of data files which in many cases will be difficult if not impossible to detect. The storage capacity of magnetic and laser disks allows large amounts of material to be easily copied and removed, and the use of communications systems allows copying and extraction of data with a low risk of detection. *Software piracy* is a problem of misuse rather than theft as the software is copied rather than stolen.

Attackers and Methods of Attack

113. **Insider**. The major single source of attack on computer systems is from personnel inside the organisation - typically employees or contractors with access to data entry or computer system facilities. Insider attacks in general are both lucrative and successful. The majority of insider attacks are not detected and, of those that are, few are reported.

114. **Outsider**. An outsider is someone not working for the department in any way and generally not having authorisation to access departmental premises or computer systems. Outsiders need to gain physical access to the computer, to gain electronic access to the computer through communications systems, or to covertly infiltrate rogue software into the system in order to mount an attack.

115. **Methods of Attack**. There are many methods of attack. Insiders can attack through legitimate access to computer systems; outsiders often attack by exploiting vulnerabilities in access control mechanisms, otherwise known as hacking. Other methods of attack include scavenging of information from discarded media, passive interception, and covert infiltration such as used by viruses. Any particular attack will exploit specific vulnerabilities of one or more targets: for instance PC viruses exploit the combination of open architecture design (vulnerability) of the computer system (target), ability to modify (vulnerability) application programs (target), lack of operational monitoring (vulnerability) of the microcomputer (target), and the common practice of exchanging diskettes (vulnerability) between systems (targets). The methods of attack will differ from department to department, depending on the sensitivity or classification of the information processed and the departmental computer system architectures.

Targets

116. An attack can be mounted against one or more of the four major targets in any computer system. These targets are:

a. **Information**. The ultimate target in most computer security incidents is the electronic information stored in and being processed by the system.

b. **Software**. Software targets include the operating system and the application programs. Attacks which target the security mechanisms built into operating system software are of particular concern.

c. **Communications**. As computer systems become more accessible through wide area networks, the networks themselves become targets. Wide area data transmission lines are not protected by physical security perimeters and are therefore vulnerable to tapping and disconnection.

d. **Equipment**. Equipment such as host computers, input-output devices, and data storage media are vulnerable to attack.

Vulnerabilities

117. Vulnerabilities occur where targets are not perfectly protected against all potential attacks. The vulnerability of a particular computer system is a product of many factors and hence two similar systems in different

departments may have differing vulnerabilities. For instance, where destruction of data by a malevolent user may be a serious vulnerability for a microcomputer located in a public room, it would be less of a vulnerability for a stand-alone system located in an access controlled computer room.

Impact of a Security Incident

118. The impact of a security incident can be described in terms of the loss of one or more of the aspects of computer security:

a. **Loss of Confidentiality**. Loss of confidentiality occurs through unauthorised disclosure of information through attacks such as media theft, interception, or misuse by hacking or scavenging.

b. **Loss of Availability**. Loss of availability occurs through either denial of service or theft of information or equipment. The system as a whole may be unavailable, or access to a particular database or item of information may be lost. This impact results from attacks such as virus and trojan horse programs, severing of communications trunks, or saturation of system resources.

c. **Loss of Integrity**. Loss of integrity occurs when software operates in a way it was not intended to, or information is incomplete or incorrect. Loss of software integrity can result from negligence or rogue software attack, and loss of information integrity can result from incorrect programs, insertion of false information, or sabotage attacks.

Protective Measures

119. Protective measures can take many forms, ranging from simple business procedures to extremely sophisticated hardware and software products. Protective measures are addressed in more detail in Chapter 4.

120. The amount of protection provided by a product or system can be assessed by evaluation within a standard security framework known as the Common Criteria for Information Technology Security Evaluation (CC). This framework also allows the strength of protection to be evaluated.

121. The basic protective measures appropriate for a computer system are selected from a set of minimum standards by considering the system architecture, the location of the system, and the sensitivity of the information being processed. Where appropriate, any further protective measures required can be determined by conducting a risk analysis to identify the remaining system vulnerabilities.

CHAPTER 2

COMPUTER SECURITY POLICY AND PLANS

Introduction

201. A policy statement defining business aims and how operational activities relate to these aims is fundamental to the management of any organisation. A set of rules (manuals, handbooks, etc) must also be available to expand the policy and show how it is to be applied. All of the aspects of management - including the application of security - need to be addressed in an integrated manner in order to ensure that departmental operations are effective and efficient.

202. Policy for the application of computer security (COMPUSEC) in government is contained in *Security In Government Departments* (SIGD), published by The Department of Prime Minister and Cabinet, and the 100 series of NZSIT publications administered by the GCSB. The basic requirements are as follows:

a. Protective measures as defined in the appropriate set of minimum standards are to be applied to all computer systems storing or processing classified information. Such systems should be accredited.

b. Protective measures as defined in the appropriate set of minimum standards should be applied to all computer systems storing or processing sensitive information.

c. Communications security (COMSEC) measures in accordance with national doctrine are to be applied to all systems processing and/or transmitting classified or sensitive information.

203. The security of information should be considered at the initial planning stage of each computer system or group of systems. Security of information should include COMSEC and COMPUSEC considerations in conjunction with the physical and personnel security measures planned for the system.

Departmental Policy

204. Each department should have a Departmental Security Policy which defines the nature of departmental activities, and documents how national security and privacy principles are to be applied. These principles should then be applied to a specific Departmental Computer Security policy.

205. The Departmental Computer Security Policy is a statement of a department's required computer security posture and should be issued or endorsed at the senior management level. The policy should be written jointly by technical and policy personnel. The minimum levels of departmental computer security should be at least as stringent as national standards, but may be more extensive.

206. The computer security policy should be a succinct statement of the overall security policies with respect to computer systems, the minimum acceptable levels of security for computer systems, and the procedures for applying computer security requirements. The policy document would typically be constructed as follows:

Chapter 1 : Executive Policy Statement

- Contents
- Introduction
- Relevant Legislation and Policies
- Information Security Philosophy
- IT Security Overview

Chapter 2 : Security Organisation

- Security Responsibilities
- IT Security Forum
- Configuration Management Board
- Security Advice and Assistance
- Outsourcing and Contractors

Chapter 3 : Asset Classification and Control

- Asset Inventories
- Information Classification and Marking Scheme
- Document and Media Destruction

Chapter 4 : Personnel Security

- Staff Trustworthiness
- Code of Conduct Agreement
- Training and Review

Chapter 5 : Physical and Environmental Security

- Secure Areas
- Equipment Security
- Protection of Cabling
- General Controls

Chapter 6 : Communications and Operational Security

- General
- Operational Procedures
- Incident Management
- Separation of Development and Operational Facilities
- Outsourcing of IT Services
- System Planning and Acceptance
- Malicious Software
- Back-up and Recovery Procedures

- Network Management
- Data Storage Media Handling and Security
- Protection of System Documentation
- Data and Software Exchange
- The Internet

Chapter 7 : Access Control

- Account Management
- Passwords
- Login Procedures
- User Access Control
- Workstation Security
- Sensitive System Isolation
- Inter-Network Access Control
- System Monitoring
- Duress Alarm
- Clock Synchronisation
- Mobile Computing and Teleworking

Chapter 8 : System Development and Maintenance

- Security Requirements
- Security in Software Applications
- Cryptographic Controls
- Operating Systems and Package Management
- Protection of the Development Suite and Test Data

Chapter 9 : Business Continuity Management

Chapter 10 : Compliance

- Management Approval Process
- Inspection and Testing

System Security Plans

207. Specific security plans should be developed for each computer system or group of similar systems (for example, administrative microcomputers could be covered by a single group security plan). These plans should define the architecture of the system, the categories of information and users on the system, indicate the risk to each aspect of the intended or actual system, state the protective measures incorporated into the system design, and set down contingency plans in case of system unavailability.

208. The security features defined in the system security plan are an interpretation of how departmental security policy applies to the system, and provide the functional criteria against which the system can be evaluated.

209. A typical system security plan should be constructed as follows:

Section 1: Basic Facts

- System Specification and Design.
- Information Classification.
- Assessment of System Security Requirements.

Section 2: Security Features.

- Security Responsibilities.
- Required Level of Assurance.
- Physical Containment and Markings.
- Personnel Security Procedures.
- Computer Security (Confidentiality) Measures: Access control, authentication of user and data origin, interconnection and electronic data exchange, electromagnetic emanations, traffic flow
- Computer Security (Integrity) Measures: Trusted software, consistency and non-repudiation, intrusion detection, communications, security monitoring
- Computer Security (Availability) Measures: Backup procedures, designed redundancy and recovery

Section 3: Configuration Management.

- Configuration Management Board.
- Change Approval Procedures.
- Baseline Documentation.

Section 4: Contingency Plans.

- Contingency Policy and System Priority.
- Key Responsibilities.
- System Configuration Information.
- Information and Software Backup Details.
- Alternate Site Agreements.
- Disaster Types and Recovery Procedures.

CHAPTER 3

APPLYING COMPUTER SECURITY

Introduction

301. Computer security measures should be incorporated into the original specification for a computer system. When security is applied retrospectively, it often costs more and is more obtrusive. A great deal of protection can be gained from well designed systems and effective procedures, and from ensuring that departmental staff are aware of the vulnerabilities of their

computer systems and that their day to day activities take these vulnerabilities into account.

302. The steps to be taken in applying protection to a computer system are:

a. Assess the threat levels for the system;

b. Incorporate the minimum departmental computer security standards into initial system specifications;

c. If justified, undertake a risk analysis taking into account initial protective measures and apply further protective measures to reduce risk to acceptable levels;

d. If required, certify that the implemented system conforms to stated security requirements;

e. If required, maintain configuration control throughout the life of the system; and

f. Review system security on a regular basis.

Threat Assessment

303. The first step in applying computer security is to assess the threat levels for confidentiality and availability/integrity for the system. In particular, the assessment should consider the attractiveness of departmental information and the likely sources and methods of attack.

304. The assessment should also seek to establish the potential damage of a successful attack in order to provide a cost basis for justifying security measures beyond the departmental minimum standards.

Minimum Standards

305. The next step in applying computer security is to establish the relevant minimum standards required by departmental policy for the system. Protective measures to meet the required security standards can then be selected. Departmental minimum standards should be no less stringent than those specified in national doctrine.

Risk Analysis and Management

306. Risk analysis, although substantially more complex and costly than using minimum standards, can be used to produce a more specific statement of security needs. A risk analysis will produce an assessed risk factor for the system as a whole and will identify specific areas of vulnerability. The risk analysis procedure involves the following steps:

a. Identify specific assets of the system such as information, programs, equipment;

b. Determine for each asset the type of security violation and potential frequency;

c. Determine the impact of each potential attack; and

d. Derive a risk factor for each asset and for the system as a whole by using the impact and expected frequency of each violation.

307. The risk analysis of computer systems can rarely be precise. It is common to have fairly broad categories of risk and vulnerability (very low, low, medium, high) rather than precise figures. There are many adequate public and proprietary risk analysis methodologies available and many automated risk analysis support systems.

308. The risk analysis process provides a list of threat/asset pairs with their associated risk factors, and an overall system risk factor. Risk management then allows the system designer to apply protective measures to each threat/asset pair in order to reduce the risk to an acceptable level. Protective measures rarely provide total protection; computer security products addressing similar vulnerabilities will often provide different degrees of protection. GCSB can provide information on the effectiveness of specific items of computer security hardware or software on request from NZ Government departments.

309. Many measures will provide protection for more than one vulnerability. The aim of a risk management methodology is to identify the combination of protective measures which together provide the most cost effective means of achieving a required level of protection.

System Certification

310. System certification is a formal method of assessing the extent to which a computer system meets the planned security level and certifying that security has been adequately applied. This should be carried out according to *NZSIT102: Certification of Government Computer Systems* . Certification is the result of a technical evaluation which establishes the extent to which system design and implementation meet the requirements specified as part of the system security plan. Certification can be performed in parallel with, or after, system development. When performed in parallel it is more apt to have accurate design documentation available; however, operational systems have

the advantage of yielding a history of security incidents. It is important to note the following points:

a. Certification can take place only if there exists an accepted system security plan identifying the specific security required.

b. Certification is a technical process which provides a judgement on the security posture of a system and is therefore a technical opinion, not a guarantee.

c. Certification can take place at departmental level and will provide the base documentation from which a system can be accredited.

311. There are five major steps leading to certification, and these are applied iteratively. Findings from one stage may cause the results of a previous stage to be reviewed, and generally elements of more than one stage will be occurring concurrently. The evaluation process can vary from a few days to several months, and it is important to ensure that a balance exists between security risks and certification costs. For this reason the process provides an overall (basic) evaluation and, where necessary, a series of more detailed evaluations of specific aspects. The main stages in the evaluation process are:

a. Planning;

b. Data collection;

c. Basic evaluation;

d. If and where required, detailed evaluation; and

e. Certification reporting.

312. Planning ensures that specialised skills, support tools, and other situation specific resources are available at the right time for the certification. Planning requires expertise in and knowledge of both the application and the certification process, and may require the enlistment of external support. Of particular significance during the planning phase is establishing the boundaries of the system to be certified.

313. A variety of data is required to carry out an evaluation. A security plan and formal risk assessment are required before the evaluation can start. The evaluation process then reviews the system against these documents, using data flow and structure charts, system design documents, and the system source code. Data can also be collected through interviews with application development and support personnel.

314. Basic evaluation involves reviewing the risk management techniques employed by the system, and aims to answer the following questions:

a. Are the stated system security requirements acceptable?

b. Do the installed protective measures satisfy all requirements?

c. Are the installed measures implemented correctly?

315. If the basic evaluation identifies any potential areas of weakness, or if any particular area of the system is particularly sensitive, a detailed evaluation of each such area should be undertaken. Detailed evaluation looks at the protective measures from three points of view: functional operation, performance criteria, and penetration resistance. Once all detailed evaluation has been completed, the evaluation can proceed to certification reporting.

316. The certification report is the primary product of the evaluation process, and contains technically based security recommendations for the system. Typically the report will contain the following:

Section 1: Top Level Specification.

- User Requirements.
- Information.
- Environment.
- System Design.
- System Management.
- Security Overview.

Section 2: Detailed System Description.

- System Architecture.
- Information Architecture and Data Flows.
- Functional Specifications.

Section 3: System Security Policy and Plan.

- Basic Facts.
- Security Features.
- Configuration Management.

Section 4: Security Inspection Reports

- Inspection Test Plan and Results.

Section 5: Certification of Compliance Statements

- Security Feature Compliance Statements.

Accreditation

317. Accreditation is the official authorisation and approval for a computer system to carry out its defined processing function within the environment in

which it was certified. Accreditation implies that the system is accepted as having correctly implemented adequate protective measures according to national security policy. National minimum standards define the circumstances under which systems will require accreditation.

318. The accreditor is responsible for evaluating certification evidence, deciding on the acceptability of protective measures, identifying corrective actions where required, and ensuring that corrective actions are carried out. On approval of the system, the accreditor will provide a formal certificate of accreditation.

319. System accreditation does not provide a whole of life approval, and may be restricted to a specific time period. In addition, re-certification and re-accreditation may be required on the basis of changes in security policies or threat assessments, changes to the system configuration, violations of security, or internal audit or review recommendations.

Configuration Management

320. Certification and accreditation provide a statement of the status of a computer system relative to departmental security policy in force at the time of the assessment. Departmental security policy should also include the requirement to implement configuration management, the process by which management controls the application of system changes to ensure that security is maintained. Configuration management also provides important input into future re-certifications, and may identify the need for a re-certification after changes have been implemented.

321. Configuration Management during development and ongoing maintenance ensures that:

a. the system operational and security policy is met by a suitable hardware configuration,

b. software undertakes the required tasks according to specifications and without undesirable side effects,

c. personnel are adequately deployed to maintain operation of the system in accordance with departmental policy,

d. changes to the system are approved and are in accordance with departmental policy, and

e. changes perform according to specification and the standard of system security is maintained.

Contingency Planning

322. Contingency planning analyses the potential incidents likely to occur in a computer system, and defines the actions required to recover from each incident. In particular, a contingency plan considers manual processing methods or standby sites as a means to recover a computer system in the event of lengthy outage or total loss. There are many commercially available contingency planning methodologies that are suitable for departmental use.

CHAPTER 4

PROTECTIVE MEASURES

Introduction

401. There are many hardware and software devices available to provide protection against a variety of attacks. A list of current approved security devices and preferred products can be obtained on request from the GCSB, and if required the GCSB can carry out investigations into the effectiveness of non-approved protective measures. This chapter provides some insight into the various types of protective measures.

402. While the use of appropriate hardware and software features can provide substantial improvements in security, significant computer security can be gained by the use of carefully designed management and control procedures throughout the life of the system. Security is maintained during software development by code reviews and, where appropriate, use of formal development techniques. Standard operating procedures should be defined, implemented, and monitored. Configuration management provides assurance that security is maintained throughout the life of the system.

403. The categories of protective measures discussed in this chapter are interdependent. For instance, if a substantial physical security environment exists, staff are cleared, and the computer system has no outside communications then the need for highly sophisticated access control software is reduced. Protective measures should be considered and applied as a whole, not separately.

Physical

404. Appropriate physical and personnel security measures need to be defined before computer security is considered. The publication *Security in Government Departments* details the protective measures that are to be applied to classified information.

405. Security container standards should be applied to computer produced documents and electronic media such as floppy diskettes and removable hard disks.

406. Sensitive or classified information output from a computer system needs to have appropriate markings, preferably incorporated onto the output by the operating or application software. Automatic labelling by the computer system is provided only by specifically designed secure computing systems, known as Trusted Systems, at higher levels of protection.

407. Media should be labelled with the highest classification of any data ever stored. To avoid scavenging, media labelled as having held sensitive or classified data should be purged using approved procedures prior to being downgraded and reused, or should be destroyed when no longer required. These procedures are detailed in *NZSIT207: The Declassification of Storage Media.*

Personnel

408. Personnel security measures should be considered for those personnel involved in computer systems. Special emphasis should be given to the trustworthiness of operators, systems programmers, and system administrators who are often given special privileges. When particularly sensitive or critical systems are being developed, departmental procedures should ensure that at least two staff are involved in system development and support.

CONFIDENTIALITY MEASURES

Identification and Authentication

409. The confidentiality of information stored in a computer system depends upon uniquely identifying all users of the system. The most popular means of doing this is by a user identification code, or userid. Userids are typically an integral part of multi-user computer operating systems, and there are many third party user identification systems available for single user microcomputers.

410. Possession of some form of token can be used to prove identity. Magnetic cards are often used as computer system identity tokens, although more exotic biometric identifications such as fingerprint, voice, palm and retina patterns can be used.

411. Userids and tokens can be stolen or copied, so when used alone do not provide adequate guarantee of the user identity. Authentication measures are therefore used in association with userids and tokens to verify the user identity. The most popular method of authentication is the use of a password, which is the electronic equivalent of a combination lock. A good password-based authentication system will typically:

a. ensure passwords are not too short,

b. limit the life of passwords,

c. not allow passwords to be re-used, and

d. lock out terminals after a number of failed access attempts.

412. Password authentication schemes are vulnerable, and easily guessed passwords such as personnel numbers or words listed in a dictionary are particularly susceptible to hacking attacks. Better password schemes use words which are in themselves meaningless but are easily remembered by an authorised user of the system, for instance the first letters of a phrase. Computer generated passwords can ensure only "good" passwords are used, and one time passwords provide a high assurance of authentication.

413. In some systems, for example funds transfer and electronic document interchange, more sophisticated authentication techniques are required. One such technique is public key encryption which uses a private key to encrypt a message and a matching public key to decrypt it. If the message can be decrypted using the public key, then only the authentic sender could have sent it.

Access Control

414. It may be desirable to use encryption techniques to protect data on storage media in transit, or to provide a second level of protection for data stored in the computer system in case primary access controls are breached. Departments should in all cases consult the GCSB on the suitability of any commercial cryptographic device proposed for the protection of government information.

415. Access control measures can be used to limit access to specific files, programs or physical devices in a computer system, and some database products provide access control down to the level of fields within the data record. Access control measures require access rights to be associated with userids, and security labels to be associated with each secured entity. Labelling schemes should also provide standard document security markings on hard copy system output.

416. The requirement for waste disposal of sensitive and classified media is no different from that for the waste disposal of classified documents. To avoid unauthorised access through electronic scavenging, electronic media that have held sensitive or classified information must be destroyed in an approved manner or be purged using approved data cleansing or degaussing equipment. Similar considerations apply where non-volatile memory chips have held classified information or algorithms.

417. Any information stored in a re-useable system resource, such as a disk buffer, must be cleared before the resource is returned to the system, otherwise sensitive or classified data could be unwittingly passed to a user not authorised to access the data. This is known as the object re-use, or data remanence, problem and protection can be provided only by the operating system.

Interconnection

418. Security in wide area communications cannot be provided by securing access to the communications lines themselves. Communications bearers are located mostly outside of the physical perimeters controlled by a department, and may use terrestrial or satellite links. Because of the opportunity for intercepting communications, encryption is needed to protect transmitted information.

419. Line or data encryption provides protection for transmitted information. Communication of classified information is governed by national communications standards, and cryptographic systems used for the protection of classified communications must be approved by the GCSB. The protection of sensitive government information should also use approved encryption systems. Departments should in all cases consult the GCSB on the suitability of any commercial cryptographic device proposed for the protection of government information.

420. The use of dial in lines or connection to public networks provides the opportunity for unauthorised access. Protection can be provided by using dial-back modems which allow only predefined telephone numbers to connect to the system or by having an operator manually establish the connection. Secure features of X.25 networks such as closed user groups can be used to provide some degree of protection, and one time passwords can prevent unauthorised access through password interception.

421. Local Area Networks generally have good physical protection by virtue of their localisation within departmental buildings. Most commercial LANs use a broadcast technique whereby all data is sent to all stations and ignored by those stations for which it is not addressed. As all data can be intercepted by a rogue terminal on the LAN, special secure LAN systems have been designed to protect against interception. External gateways on LANs also need to be carefully selected so as to provide adequate access controls from external sites.

422. Computer systems are increasingly being connected together and configured for automatic machine to machine communications. Each computer needs protection to avoid inter-system attack from other connected computers. Classified systems may be connected to each other only through transmission paths protected by approved encryption devices.

423. Where information needs to be transferred between systems that either require isolation or have different security levels, the connection should be

through an approved filter (a trusted computer system), by data transfer using exchangeable media such as tape or diskette, or by re-entry from hard copy.

Electromagnetic Radiation

424. Computer systems, communications equipment and peripherals are all potential sources of compromising radiation. Departments should contact the GCSB for advice if minimum standards or a subsequent risk analysis point to the need for protection from this form of attack.

425. Fibre optic cable can be used to avoid the emanations associated with metal cable, but it can still be tapped through cohesive detection techniques unless special anti-tamper fibre is used.

Traffic Flow

426. Information can be deduced from the levels of traffic flow between source and destination points. Traffic flow protection can be provided by padding traffic with synchronisation messages.

427. Routing tables can be used to ensure classified information is transmitted only on communications channels cleared for handling such information.

INTEGRITY MEASURES

Start Up Self-Test

428. While a system will have a defined level of integrity when initially installed, integrity throughout the system's life can be assured only through ongoing integrity checks. The integrity of hardware is assured by power on self testing; the integrity of software by some form of program hash check either before startup or as part of software initialisation.

Consistency

429. Consistency of information held is an important integrity property for any computer system. Controls for integrity checking include the application of transaction rollback to recover from incomplete updates, and online database update logging.

Non-Repudiation

430. It is important to have a guarantee of message origination for systems such as electronic ordering systems where actions are accountable. The guarantee that a message originator cannot subsequently deny originating the message is known as non-repudiation of origin, and can be achieved using digital signatures. A similar guarantee that a message has been received is known as non-repudiation of receipt and can be provided by a digital signature as part of delivery notification.

Intrusion Detection

431. Diskless workstations or terminals provide good protection from insertion of rogue software such as viruses and trojan horses. However, they do not provide complete protection against intrusion as a competent and determined attacker can enter an item of rogue software by keyboard entry.

432. There are available many anti-virus software packages which provide good protection against virus attack. Such software works in one of two ways - either by continually monitoring all activity on the system and detecting what is considered to be an anomaly, or through operator initiated scanning of the system to check for viral signatures. However, the most effective protective measures against viruses are good management techniques, which include:

a. checking all foreign media before importing programs or data,

b. keeping regular backups of data, and

c. controlling access to system input devices.

433. As a further level of protection in the event of failure of access controls, systems can provide levels of intrusion detection. The most common is the provision of an audit trail so that breaches of security can be tracked down after the event to determine the originating time and place. Some monitoring systems provide real time intrusion detection, as in the case of anti-virus products which monitor for abnormal activities or known attack signatures.

434. A commonly used mechanism for identifying an intrusion after the event is to maintain an audit trail of system activity in the form of a security log. Most commercial systems have system logs of some form and many have specific security logs. Third party systems for access control frequently include security audit facilities. The most important aspect of a security audit trail is ensuring that it is well protected against attack.

Communications

435. Communication systems have integrity checking and error recovery built into their communications protocols. The two common techniques are checksums on communications packets and message sequencing.

AVAILABILITY MEASURES

Backup Procedures

436. Regular backups and off-site storage are traditional measures used to protect the availability of information stored in computer systems. In the event of corruption of data or total loss of the system, data that is both recent and correct to a defined point in time can be quickly re-established for use. Typical backup regimes include daily backups of changed files (incremental backups), and weekly full backups of the total database.

Designed Redundancy and Recovery

437. Modern computer systems may include designed redundancy to allow continued operation albeit with reduced performance. Examples of this are multi-processor systems, mirrored disk subsystems, alternate communications routing, automatic error correction, and link recovery.

CHAPTER 5

SECURITY OF SPECIFIC SYSTEMS

Microcomputers

501. IBM-compatible microcomputers are designed as single-state machines with no privileged instructions, allowing any machine operation to be performed by any user. The design of the Microsoft DOS and Windows (3.x, 9x, etc) operating systems also follows this single-state paradigm to provide a single-user operating system with little concept of user and process separation. Many other microcomputer systems are also single-state/single-user.

502. Microcomputer security systems cannot therefore use inherent operating system features, and so must depend upon third party products which extend the operating system in areas such as identification, authentication, access control, file encryption, and secure deletion. These products provide security features through either software alone or software and hardware in combination.

503. Software only access control systems can be circumvented by booting from a floppy diskette. To avoid this, some third party products provide boot

protection through controlled corruption of the partition table. However, a skilled attacker can readily build a replacement partition table.

504. Hardware based products invoke security measures regardless of the boot process, but removal of the hardware device may be sufficient to circumvent the security features.

505. The confidentiality of information held on microcomputers can be protected by using removable disks and normal document security doctrine. Protection for information stored on fixed disks can be provided through encryption.

LANs

506. Most LAN systems consist of standard architecture IBM-compatible hardware with network interface cards, a network operating system on the file server, and Microsoft, Linux or Apple operating system software on the terminals. All data is broadcast around the network to every terminal, and is ignored by all but the terminal for which it is intended.

507. LAN terminals have the same level of vulnerability as microcomputers. In addition the network is vulnerable to a rogue terminal intercepting any or all of the data being broadcast. Identification, authentication, and access control facilities are generally available to protect LAN resources, but in most cases they need to be activated by the system administrator.

508. LANs can be designed with security in mind by using diskless terminals which boot from an internal ROM. This provides protection against virus infiltration and unauthorised extraction of datafiles. This protection is only as good as the physical security of the LAN, as workstations can be easily modified or replaced.

UNIX Systems

509. The UNIX operating system is designed to incorporate identification, authentication, access control, and object reuse. However, the open architecture and public availability of the UNIX system design and code has allowed many loopholes to be identified and exploited. Protection can be applied to UNIX systems by careful management of system security features and an awareness of how to avoid identified security loopholes.

510. Some high-assurance versions of UNIX provide additional security features such as labelling for access control and trusted login paths. Several of these have been tested to meet the requirements of E4 / EAL5 level assurance.

Proprietary Systems

511. Many proprietary systems have security features built into the operating system and enhanced security packages that can be installed. Such facilities can generally provide good levels of security, but often fail because of inadequate administration. A common failing is to leave vendor default user identifiers and passwords activated.

CHAPTER 6

PROCUREMENT OF COMPUSEC ITEMS

General

601. When departments need to procure items of computer security related hardware and software from overseas, the GCSB can offer assistance in ensuring the purchase goes smoothly through overseas export approval procedures. Departments should contact the GCSB for advice on procurement of any computer security product. Procurement procedures can be expedited by the GCSB in all cases, but in particular for:

a. TEMPEST equipment,

b. hardware or software involving any type of encryption, and

c. trusted software.

602. A number of computer security products can be purchased for normal commercial use, or with special options for government use, and third party vendors sourcing such products from overseas may not be aware of these special options. When considering procurement of any computer security products for sensitive or classified use, departments should contact the GCSB for further information.

CHAPTER 7

LIAISON, REPORTING AND ASSISTANCE

Liaison

701. For computer security matters, the normal IT security contact in departments is the Departmental Security Officer (DSO). Some departments may wish to delegate the computer security liaison function to a specific Information Technology Security Officer (ITSOs).

702. From time to time GCSB may coordinate computer security working group meetings of DSOs/ITSOs to discuss computer security issues and provide a forum for interdepartmental discussions.

Reporting

703. Any acts of espionage, sabotage, terrorism, or subversion involving COMPUSEC violations are to be reported to the GCSB. Departments should also report any other computer security attack so that vulnerabilities can be identified and other departments notified accordingly.

Assistance

704. The identification and resolution of COMPUSEC incidents is the responsibility of the department concerned. Where it is beyond the capability of individual departments to resolve the incident, the GCSB will provide advice and assistance within the limits of available resources.

705. The GCSB on request is able to provide advice and assistance to Government departments in development of computer security policy, application of computer security, evaluation of products and systems, and approved protection measures; however, the GCSB does not generally provide specialist advice on issues such as backup, disaster recovery, electronic vandalism and fraud unless classified information is involved.

706. Requests for advice or assistance in any area of computer security should be made in the first instance to the Director, GCSB.