New Zealand Security of Information Technology Publication 200

THE SECURITY OF PERSONAL COMPUTERS

CHAPTER 1

THE PERSONAL COMPUTER ARCHITECTURE

General

101. The computer system most commonly used in Government is the Intel x86 based microcomputer running Microsoft Windows software. This system is referred to as the Personal Computer (PC). The first PC system was developed in the late 1970s by an entrepreneurial division of IBM as a small computer useable by non-technical staff for word processing, spreadsheets, and other small business tasks. IBM made details of the hardware and software architecture widely available in order to encourage the development of third party hardware and software subsystems.

102. At the time PCs were first developed, mainframe computer architectures provided inherent separation between users and the hardware environment through operating system controls. This separation, which is fundamental to mainframe security, was not considered practicable or necessary for single-user systems such as the PC. The initial PC Disk Operating System (DOS) was designed to provide adequate functionality while minimising the use of memory space, and appeared primitive when compared to the mainframe and minicomputer operating systems in use in the early 1980s. The subsequent development of the Microsoft Windows system provided a substantially more useable interface for many non-technical users, while initially retaining the same fundamental operating system concepts. Since then, more sophisticated PC operating systems such as Windows-NT and Windows 95 have been introduced to provide increased functionality at the operating system level, and to isolate users from the technical operation of the PC. Now, mainframe and minicomputer operating systems appear to be primitive when compared to these systems.

103. Since the introduction of the IBM PC in the early 1980's, use of the PC has become widespread in the private sector and in the home, and the PC is now the platform of choice for much of the information processing within Government. As with any technological advance, the risks associated with the use of PCs need to be recognised and minimised by the selection of appropriate countermeasures.

104. 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. The Privacy Act 1993 requires that personal information be protected from unauthorised disclosure and use, and that proper procedures be followed for data matching between departments. In some cases further protection of information may be required as a result of specific legislation relating to the department or the policies adopted by the department.

105. The purpose of this publication is to provide Government managers and users with an understanding of the security problems associated with PC use, and with national doctrine on the security measures recommended for the protection of official information stored and processed on PCs. While this publication provides guidance on security in DOS/Windows PCs, many of the issues raised are relevant to other types of small single user computers and operating systems. The GCSB will provide specialised advice on securing other types of microcomputer systems on request.

PC Architecture

106. From a physical perspective, the main components of the PC architecture are the PC motherboard, the motherboard adapter cards, and any connected peripherals such as the monitor, keyboard, mouse, and printer. PCs are fielded in one of three forms: network servers, desktop workstations, or notebook computers. In all cases the hardware architecture is similar, although notebook computers are, of course, designed with severe size and weight constraints. The software configuration is similar in notebook and desktop computers.

107. Network servers are usually configured with server software such as Windows NT Server or Novell Netware, and tend to be fielded in more secure areas under the control of a network administrator. The security of network servers is a subject in its own right and is not considered further in this publication.

108. The main PC circuit board, called the motherboard, contains the following core PC components:

a. the processor and integrated circuits (ICs or chips) which support its operation;

b. the random access memory (RAM) required for program execution;

c. the read-only memory (ROM) containing the basic input/output firmware (BIOS) which interfaces at the hardware level between software and the motherboard hardware;

d. slots for the electrical connection of adapter cards; and

e. a small non-volatile memory for the storage of configuration data (usually referred to as the CMOS). This is associated with the real-time clock IC and may on some systems be used to store a power-on password and parameters controlling the start-up (boot) sequence.

109. The connector slots in the motherboard provide connections to the computer data bus for a wide range of adapter cards. The typical cards used in PCs include:

a. video controller logic and additional video memory, to enable program output to be displayed on the monitor screen;

b. diskette drive and hard disk controllers, to provide access to magnetic storage media;

c. serial ports to enable communication between software and peripherals such as a pointing device, printer, or modem;

d. parallel ports to allow connection of a printer;

e. network interface cards; and

f. special function cards such as scanner interfaces, data acquisition or signal processing cards, and sound cards.

110. The disk controller circuitry may be located on an adapter card or, in some systems, directly on the motherboard. This circuitry is used to handle the low level functions required for a disk to store and retrieve data. Newer types of hard disks often implement some of this computational processing into the disk drive itself to increase throughput. The disk drives onto which data is stored are usually located in a drive bay within the computer case and connected to the disk controller through ribbon cables. PCs can alternatively be configured with removable hard disks in a variety of forms, including PC cards.

111. The serial port may be used to connect directly or through a modem into a host computer. The PC can emulate a serial terminal or, using advanced communications protocols such as Point-to-Point Protocol (PPP) or Serial Line Interface Protocol (SLIP), operate as a networked host computer in its own right. PCs can also be configured with a network adapter card to enable connection to a local area network.

112. From a more conceptual perspective, a computer consists of a processing unit, a memory subsystem, a disk subsystem, I/O devices, operating system software, and applications software. These subsystems logically encompass various hardware components and software modules. Security needs to be considered from both the architectural and the conceptual perspectives.

Operating Systems

113. Microsoft Windows is the most commonly used operating systems on the PC. But, regardless of the operating system used, the initial PC start up process is basically the same. The operating system specific aspects come into play once the initial program load process, or bootstrap, completes.

114. During system initialisation, a special table is set up in memory to assist in the management of the operating system and various hardware devices. This table is known in PC operating systems as the Interrupt Vector

table, and each entry indicates, for a range of interrupt-driven requests from the operating system or hardware, the location in memory of the process which is to be called to action the request.

115. Hardware interrupts are implemented through direct electrical connections to the peripheral circuitry. A peripheral gains the attention of the processor by altering the voltage level on an interrupt line, causing an interrupt request (IRQ). Commonly, peripheral cards can be configured to use one of a range of interrupts, e.g. serial port 1 generally uses IRQ3 but may be configured to use IRQ4. Software interrupts are used by the operating system processes to manage or control processor activity.

116. Application programs make use of standard system call facilities to access operating system services, particularly those associated with the input and output subsystems. These system calls are managed by what is known in DOS as the Basic Input Output System (BIOS), a set of services provided in the PC in the form of a read only memory chip known as the 'BIOS ROM'. However, for performance reasons, applications can still be written to work directly with hardware controllers and devices, in effect circumventing BIOS management.

Boot Sequence

117. When the PC is started, control is automatically passed to the BIOS software. The BIOS software performs the following functions:

a. The user can elect to enter the BIOS configuration setup program.

b. The user may be prompted to enter a power-on password as a form of access control to the system. This will be checked against the password stored in CMOS.

c. Support chips such as the timer and direct memory access chips are initialised.

d. RAM is initialised and tested, with the amount of memory tested being displayed.

e. BIOS contents may be copied into memory for better performance.

f. Interrupt vector tables are set up in memory.

g. Any BIOS extensions, such as those associated with video cards and certain hard disk controllers, are loaded and executed to enable device initialisation to take place. Extension BIOS programs will usually modify interrupt vector tables so that hardware events in which they are interested will be passed to them for processing.

h. The BIOS then attempts to load an operating system. The first diskette drive will be checked for a Master Boot Record (MBR). If no diskette is loaded, then the second diskette drive will be checked followed by the hard disk drive (or drives, if more than one are present). Some BIOS chips make provision for the user to nominate the sequence in which drives are searched: this can assist in providing protection against the introduction of viruses from diskettes by ensuring that the hard disk is accessed before the diskette drive. Once a valid MBR has been found, control is passed to it.

i. The MBR program interrogates an associated partition table to locate a bootable partition. If one is found, the first sector (by definition, this is a program to load an operating system and is called the boot sector) is executed. If no bootable partition is located, the MBR causes an appropriate error message to be displayed and the boot process will be halted. In some multi-operating system configurations, the first sector is a boot loader which allows menu selection of the operating system to be loaded.

j. The boot sector will then load its associated operating system software into memory and the operating system proper will start.

DOS

118. Once the bootstrap process has loaded it, the DOS operating system starts by looking for the CONFIG.SYS and AUTOEXEC.BAT files. The CONFIG.SYS file contains parameters which inform the operating system about preferred operating system options and may also identify specialised driver programs to be loaded and made resident, e.g. mouse drivers, video display drivers, and device drivers for non-standard media such as SCSI hard disks, and CDROM drives.

119. DOS then checks whether an AUTOEXEC.BAT batch file exists and, if so, runs it. AUTOEXEC.BAT is a normal DOS batch file which can contain any operating system commands or application programs, and is usually used to provide further details of system configuration (for example, the PATH variables are set from parameters supplied in this file). It also provides a facility for loading and executing application or terminate-and-stay-resident (TSR) programs. Most DOS menu systems are loaded from this file, and the Windows system, if used, is commonly started as the final task of the AUTOEXEC.BAT file.

Windows-NT, Windows 9x

120. In Windows-NT and Windows 9x, the system configuration is controlled through an operating system database known as the Registry. This provides many operating system and application package software settings. The programs required to be run automatically at initial startup are held in a Startup group.

The Objectives of PC Protection

121. Protective measures for desktop and notebook PCs are aimed at providing:

a. confidentiality, through protecting against unauthorised disclosure of information stored on the PC hard disks or diskettes and processed by the PC;

b. integrity, particularly through guarding against unauthorised modification of the operating system, applications software, and data; and

c. availability, through provision of an adequate contingency and backup regime to ensure that access to information can be maintained despite system failure, accident, or attack.

PC Security Standards

122. The publication *NZSIT 103: Security Evaluation Criteria for Government Computer Systems* describes predefined functionality classes for a range of computer system architectures, including microcomputers. The PC predefined functionality specification provides a class of computer security standards that, when applied, will provide an adequate level of security for stand-alone personal computers. These standards are, progressively:

a. PC0 Operating system and application integrity

b. PC1/Basic Operating system and application integrity, and access control suitable for a secure environment

c. PC1/Strong Operating system and application integrity, access control suitable for an insecure environment, and hard disk encryption

123. A further set of standards, PC2, provides security specifications for microcomputers configured for data communications.

CHAPTER 2

SECURITY MANAGEMENT PROCEDURES

Introduction

201. Information systems security is best managed through the use of formal certification and accreditation procedures. These procedures, detailed in *NZSIT 102: Certification and Accreditation of Government Computer Systems* ,

are designed to ensure that the correct security posture is identified for the system and that the security measures applied are adequate throughout the life of the system.

202. Certification is the term used to describe the development and maintenance of security documentation for an information system, and is the responsibility of a certification officer. The main documents developed during certification are the System Security Policy, the Security Plan, and the Standard Operating Procedures.

203. Accreditation involves an independent review of the certification documentation and site inspection of the system to ensure that the security measures implemented in the system meet the required level of security for the information being processed.

System Security Policy (SSP)

204. The SSP identifies the relevant security criteria as laid down in department regulations and any additional requirements identified during review or formal risk analysis of the system. It should address the physical environment and the protection required for containment of system output and media, the clearances required for staff to use the system, the protection required for interconnection of the system with other systems, and specific computer security measures such as access control or disk encryption. The Policy should also identify all staff responsible for some aspect of security on the system.

205. In order to minimise the effort involved in the administrative process of providing PC security, it is preferable to have a single, common PC security policy that identifies a standard departmental or divisional configuration and a common set of security countermeasures. An annex to such a standard policy can be used to address any special requirements of individual systems.

Security Plan (SP)

206. The SP details the specific security measures and products needed to satisfy the security requirements detailed in the SSP. Often the selection of security measures will require a balance of cost, convenience, and the impact of compromise. These considerations should be detailed. The SP will usually include a range of physical, personnel, and technical solutions.

207. Again, a common plan should, where possible, be used to minimise the administrative effort involved in documenting system security measures.

Standard Operating Procedures (SOPs)

208. SOPs are a commonly used method of documenting detailed instructions on the management and operation of a system. SOPs are particularly important for PCs as they provide specialist guidance on system management to non-specialist users. SOPs should include those procedures, such as backup regimes, relevant to security.

Inspections

209. While security policies and plans provide a documented regime for protection of official information stored and processed in PCs, periodic technical system inspections will be required to ensure that a system is secured according to its SP. An inspection will include an assessment of the threats to the system, a review of the security features of the implemented system against the documented SP, and an integrity check of the PC.

CHAPTER 3

THREATS, VULNERABILITIES, COUNTERMEASURES

General

301. The PC was originally designed without reference to any security features. The unexpected burgeoning use of PCs in critical systems and for the processing of sensitive official and commercial information has exposed a range of vulnerabilities in PC equipment. The information stored on a PC will often represent a significant resource that may be critical to departmental operations. While normal management procedures are required to minimise the impact of any accident or natural disaster, PCs should also be protected against attacks resulting from unauthorised physical access, malicious software, use of modems, and Local Area Network (LAN) connectivity. There are many known technical methods of attacking PCs, and new attacks continue to be reported.

302. Magnetic storage media is to be protected according to document storage regulations as promulgated in the publication *Security in Government Departments* . In particular, PCs must be stored, when not in use, in the appropriate form of container for the particular grade of site and classification of information held on the computer. It should be noted that the classification of magnetic storage media is to be the highest classification of any document that has ever been stored on the media, whether or not it has subsequently been deleted.

303. The use of approved encryption systems can provide an alternative to physical containment of computers. The GCSB is responsible for approving all cryptographic systems used in Government and should be consulted prior to the adoption of any cryptographic system for the protection of official information.

304. There are many security products for PCs on the market, but their effectiveness varies. Departments should contact the GCSB for advice regarding suitable products for the protection of official information.

I. ENVIRONMENT

Atmospheric Conditions

305. Traditional mainframe systems are operated in environments which provide strict maintenance of the necessary temperature and humidity levels. There are generally no special environmental requirements for PCs, but manufacturers may specify recommended temperature and humidity operating ranges. Systems are vulnerable to airborne dust particles such as smoke, and PCs which are moved regularly, such as notebooks, are vulnerable to damage through accidental bumping or dropping. PC equipment should operate without problems in normal office environments. Some manufacturers offer special ruggedised versions of their systems for use in very hostile environments.

306. PC equipment should always be operated in accordance with the manufacturer's recommendations.

Power Supply Problems

307. PCs are vulnerable to power supply disturbances which can cause unexpected shutdowns with resulting loss of data, and in extreme situations can damage hardware components. While such occurrences tend to be rare, corruption of data bases can prove difficult to remedy. A more common power supply problem occurs when PCs share a mains outlet with interference generating equipment such as laser printers, photocopiers, or shredders. Industrial electric motors are a particular problem in this respect.

308. PC equipments are designed to operate from any mains outlet. If problems occur, they may be minimised by use of a dedicated power line from the mains distribution board to the PC. Where the continuing operation of a system is critical, an Uninterruptable Power Supply (UPS) should be used.

Food and Drink

309. PCs are vulnerable to damage from food crumbs or spilled drinks. Fluid spills in high voltage equipments are likely to cause irreparable damage or even fire, and on keyboards will cause corrosion of the contacts and unreliable operation. Food or drink spilled onto diskettes are likely to cause damage not only to the diskette but also to the diskette drive.

310. Food and drink should not be consumed near PC equipment. Sealed, membrane keyboards should be used in environments where fluid spillage is likely to be a problem.

II. PHYSICAL ACCESS

Theft

311. The ready market for PCs and their components makes them attractive targets. Theft of a PC does not only represent a financial penalty and the loss of a department asset, but could also mean irrecoverable loss of data or disclosure of sensitive information. The risk of theft can be minimised by installing PCs, wherever possible, in areas which have some form of physical protection such as doors that can be locked when staff are absent. Intrusion alarm system sensors, stand-alone or linked into an office-wide intruder alarm system, can be used to detect the physical movement of a PC. There are also a variety of lock-down devices available for attaching PCs to desks. Notebook PCs are particularly vulnerable to theft when they are used outside controlled office areas.

Tampering

312. PCs are not designed with built in access controls and may be readily operated or tampered with by anyone gaining physical access to the system. PCs configured with a software access control system are still vulnerable to unauthorised access, as attackers can boot the system from their own diskettes and access the hard disk using readily available disk reading utilities.

313. Unauthorised use of departmental systems may introduce viruses or other rogue software into the system, and may result in unauthorised disclosure or damage to departmental information. PCs sent out for repair will be accessed by technicians who can not only read the information currently stored on the system, but also have the skills to recover a great deal of information that has been previously deleted from the system unless approved sanitisation procedures have been followed (see paragraph 331).

314. PCs may be designed with a physical lock to prevent operation of the power switch or to disable keyboard operation. Such locks are usually trivial to pick, and they can often be disabled by simply removing a wire from the PC motherboard. They do not provide effective security for PCs containing official information.

315. The use of CMOS power on passwords will not provide adequate protection for PCs as the password can be removed by switching the password facility off by resetting the CMOS configuration. This can often be achieved by simply removing the CMOS battery. CMOS passwords do not provide effective security for PCs containing official information.

316. A range of approved commercial access control subsystems is available for use with PCs. These can be categorised as either software-based or hardware-based subsystems. Software access control systems generally

require the entry of a user identifier and password. Hardware based access control systems may come in the form of an add-in board, dongle, smartcard, or PC card. Some hardware schemes are able to be circumvented by merely removing the hardware device, but most use some form of disk encryption to ensure that on removal of the device the system 'fails safe'. Hardware devices such as dongles and smartcards offer an additional level of security, as they can be carried by the user rather than left with the PC. However, unless also providing disk encryption, such products are of use only within secure environments and are not recommended for the protection of official information.

III. LOGICAL ACCESS

Booting

317. PCs, regardless of their operating system, are designed to allow booting from a floppy disk. Consequently, a secured system can be attacked by loading a simple DOS operating system from floppy disk, and then modifying any part of the hard disk, including the system's normal operating system. Software based security schemes designed to limit user access to PC facilities can be circumvented by this method. Even systems which claim to disallow access to the hard disk are easily circumvented using relatively simple software.

318. In a networked environment, it is strongly recommended that diskless workstations are used. This will protect against unauthorised booting as well as the inadvertent introduction of malicious software. Alternatively, boot protection security should be provided through a GCSB-approved security product.

Discretionary Access Controls

319. PCs are commonly shared between users or passed on from one user to another, often downwards through a departmental hierarchy. Whenever a PC is available to more than one user, any fixed disk storage will be accessible and vulnerable to scavenging by all users, and it is common for a substantial amount of residual material to be left on transferred PCs. In the event of equipment failure, PCs are commonly sent off-site to a dealer for repair or disposal. The information stored on the hard disk is similarly vulnerable to scavenging, even in cases where the hard disk itself is the faulty component. A similar problem occurs when older systems are sold or traded in. DOS contains no built in facility for auditing system use so unauthorised access is unlikely to be detected.

320. Mainframe computer systems implement their protection schemes at the hardware level to ensure that application users are appropriately restricted in what they may do. Smaller host computers, such as UNIX systems, implement protection in the operating system kernel, a small and trusted

central component of the operating system. The kernel enforces what is known as a privilege scheme. It operates at the highest level of privilege to allow access to all memory areas and to all instructions, while there are typically a number of lower privilege levels for other operating system functions. User application programs run at the lowest privilege state to ensure that user access is strictly circumscribed.

321. PC hardware and operating systems are not designed with privilege states, and all tasks run on the system may access all memory areas and instructions. Any program can write to the MBR, boot sector, or operating system files on disk. This allows the introduction of untrusted software into the PC operating environment, a vulnerability successfully accessed by viruses. Such uncontrolled access to all areas of the system also allows application programs to modify or corrupt themselves or the operating system.

322. DOS provides only basic mechanisms to limit user access to information stored on magnetic media using attributes associated with each file that mark it as Hidden, System, or Read-only. However, in the normal DOS environment these attributes can easily be changed by any program. Information held on storage devices can be accessed through the BIOS, or may be directly accessed by using the controller card low level interface. This makes it difficult to implement even rudimentary authentication and access control schemes.

323. While some application programs provide file passwords and data encryption capabilities, their effectiveness cannot be trusted unless the applications have been formally evaluated and included in the *NZCSIM 402 Pt 2: Preferred Products List* . In particular, encryption products which are readily available have often been configured with weak encryption modules. Where government variants of such products exist, they should be used.

324. Some newer desktop operating systems, in particular Windows-NT, provide a more controlled environment based on a form of security kernel known as the 'Trusted Computing Base' which does provide some operating system protection. Access to files by users is managed through an approved set of discretionary access controls and comprehensive auditing facilities can be configured.

325. It is strongly recommended that PCs used to store and process official information are operated under an approved computer operating system which provides discretionary access controls.

Data Remnants and Spillage

326. While the deletion of a PC data file, or relinquishment of a temporary file, will cause the file to be deleted, this does not remove the data in the file but merely removes the file name from the disk directory. The original content of these files will remain intact until the space occupied by the file contents is reused by another file. Deleted files are easily recovered by technically knowledgeable personnel. In a similar way, the DOS FORMAT command,

commonly thought to clear data from magnetic media and prepare it for use, will not always erase existing information.

327. The use of temporary disk files is another source of vulnerability. Temporary files are often used to save timed backup copies of files while word processing, and as a holding area for information prior to being sent to the printer (these are known as spoolfiles). Information can also be stored in the Windows swap file, an area of disk used to store memory contents when users switch from task to task. In all cases, relinquishment of the temporary disk area leaves the data on the disk until subsequently overwritten.

328. When a program requires space for the creation of an output file, an initial allocation of disk space, called a cluster, is reserved for the file by DOS. If more space is required as the file creation proceeds, further requests to DOS are made and additional clusters allocated. In practice, the length of a data file is arbitrary and when the file is complete an end-of-file marker will be written at the end of the data. However, the file usually occupies less than all the space available in the final cluster and the remaining space in the allocation unit, the caudal area, will contain whatever happened to be in memory at the time the file was written, as well as some information that was originally on the disk space reserved. While this information is not available to standard DOS programs, it may easily be viewed by special utility programs. As the size of the allocation unit increases, the probability that compromising information may be held in the caudal area increases. In the worst case, where a cluster contains eight sectors, more than four thousand bytes of information may be invisibly appended to a file.

329. It is mandatory that PC equipment containing classified information be either:

a. stored in approved containers as detailed in the publication *Security in Government Departments* ; or

b. use an approved, medium grade (for up to and including SECRET) or high grade (for TOP SECRET) disk encryption system.

330. It is recommended that PC storage equipment containing unclassified but sensitive official information (with priority being given to equipment located overseas) be either:

a. stored in a locked container (this can be achieved by the use of removable hard disks or containment of the complete PC);

b. use an approved, commercial grade access control system; or

c. use an approved, commercial grade disk encryption system.

331. It is recommended that the GCSB's XR25 utility, or an equivalent approved utility, be used to sanitise the disk subsystems of PCs used to store and process official information of any sensitivity. XR25 is available to NZ Government departments at no cost from the GCSB, and is fully described in

the GCSB For Official Use Only publication *NZSIT 209: Computer Security Utilities* .

Malicious Software

332. The ease of physical access to PCs, combined with the lack of adequate access controls, offers an opportunity for direct insertion of malicious software into the computer through the floppy disk or directly through the keyboard. The common practice of sharing information and programs on disk or through networks is one of the principal ways of promulgating viruses and other malicious software.

333. A virus is a computer program created to infect other programs with copies of itself. The virus has the ability to clone itself and constantly search for vectors through which it can reach new hosts. The virus will typically be attached to an executable program or exist as part of the executable boot code which must be executed for the virus to promulgate. Some viruses can use data files such as Microsoft Word documents as vectors by which they promulgate and infect systems (in this case, macros within the document effect the infection when they are executed).

334. A trojan horse is a piece of software that purports to be a known, legitimate program but in fact is a variant of, or replacement for, that program. Trojan horse programs are normally promulgated through initial placement on public network bulletin boards or file transfer (FTP) sites and subsequent copying by network users.

335. Checksums can be used to verify that key system files and executable programs have not been modified by a virus. Typically, such programs generate checksums of the required files when the system is in a known virus-free state and store then for future reference, and a program is then provided which verifies the checksums every time the PC system is booted.

336. Diskettes should be protected against inadvertent hosting of a virus through use of the write-protect tab (on 3.5" media) or covering the write-enable notch (5.25" media).

337. It is recommended that disk scanning procedures be implemented to check all incoming and outgoing media, including CD-ROMs, and that departmental users be discouraged from down loading executable code from public networks. It is strongly recommended that anti-virus software is put onto all PCs and used for periodic scanning and monitoring incoming and outgoing files.

IV. PC COMMUNICATIONS

LANs

338. Any link into a PC is an additional route by which unauthorised users can access disks and other media. The communications path may be local or remote. A local link may connect either to another PC in a nearby location, or to a local area network. A remote link may be used to bridge between local networks through a modem, providing logical access to the remote network as though it were a local resource.

339. Sensitive information held on a networked PC may be compromised in a variety of ways. When a PC is powered on and communications software and hardware are active, information on that PC can potentially be accessed from other computers without the authority or knowledge of the owner of the information.

340. Information being processed on a PC and stored on a network drive will be broadcast to all users on the LAN. Steps should be taken to isolate sensitive portions of the LAN or use approved data encryption products to protect LAN communications.

Remote Communications

341. Where remote access facilities are introduced into PC equipment, there is a risk that unauthorised access to the PC may occur. This can lead to the compromise of information stored on the PC or, in the case of networked PCs, of information stored on network servers.

342. Hardware and software solutions have been developed which allow only authorised users to dial into a system. For example, a call-back device will require a dial-up user to supply a user identification code and password for verification by a port protection device on the target PC. The call-back device will then disconnect the caller and redial the predefined telephone number of the user associated with the identification and password supplied. Another mechanism used is the challenge-response system whereby the caller is provided with a challenge in the form of a number, and the response has to be a matching number based on some form of cryptographic process or synchronised random number. Further details of these solutions are provided in the GCSB publication *NZSIT 204: Authentication Mechanisms* .

343. It is recommended that remote access to PCs be controlled through the use of approved challenge-response or call-back systems.

344. Electronic bulletin board systems are primarily operated by personal computer user groups and hobbyists and offer information, software, games, and news items to those with access through dial-up telephone lines. However, they can often contain objectionable material, pirated software, and malicious software.

345. It is recommended that departments do not allow access to bulletin boards from departmental computers.

V. OTHER ISSUES

Compromising Emanations

346. PCs can produce emanations (in the form of electromagnetic radiation (EMR) over a wide band of frequencies) which contain sufficient data about the information being processed to allow its unambiguous recovery. These emanations can sometimes be retrieved by an unauthorised individual located some distance from a PC, with no indication to the user that the information has been compromised.

347. EMR can be carried through free space, by communications lines, by power lines, or by other conductors attached to, or close to, the system.

348. The use of GCSB approved equipment, or the establishment of adequate secure boundaries, can reduce the risk from these emanations to an acceptable level. The GCSB can assist departments in assessing the risk and in selection of suitable countermeasures.

CHAPTER 4

BACKUP PROCEDURES

Backup Strategy

401. Information stored on magnetic media is vulnerable to degradation and to accidental corruption or deletion, and backup copies of electronic documents should be made at suitable intervals. The method and frequency of file backup is best determined by each user against general departmental guidelines and should be based on the type of storage media and the volatility of the information involved.

402. For data stored on removable media, the entire volume should be copied after each use or, if the volume is in frequent use, at the end of the working day. This approach eliminates the need to keep track of each individual file. If the original volume is damaged then the backup can be used. For critical applications it is often wise to retain two backup volumes, one containing the previous day's work and a second which is two days old. By using the older volume for the new backup medium a two day backup cycle can be maintained.

403. For large capacity storage devices such as fixed disks it may be too cumbersome to perform a full disk copy on a daily basis. In this situation, you should consider the use of incremental backups or application backups. The use of RAID (Redundant Array of Inexpensive Disks) technology should also be considered.

Incremental Backup

404. In an incremental backup, only those files which have been modified since the last incremental or full backup are copied to the backup medium. This requires a mechanism in the operating system to set an indicator whenever a file is opened for writing. Most personal computer operating systems which cater for hard discs have such facilities so the task can be automated. It should be noted that full backup is required at regular intervals (say monthly) for complete recovery as no single incremental backup will contain all of the files.

405. Recovery from minor problems (e.g. an error in a single file) involves locating the latest incremental backup and reloading the file. Recovery from a major problem may require rebuilding the system completely. In this case the last full backup is loaded first and then each of the latest incremental backup volumes is reloaded. This can be very time consuming and error-prone if there are too many incremental backups between each full backup. A reasonable schedule could be a full backup each month and an incremental backup each week. However, a specific schedule should be determined for each system as part of the overall policy for its use.

Application Backup

406. Because of the complexity of incremental backup and the impractical nature of full backup for large capacity volumes, it may be more appropriate to consider backup based on each application or file grouping (e.g. file subdirectories). Certain file groups (e.g. applications software) which rarely change would require only infrequent backup. Data files should be backed up whenever they are updated or on some regular schedule. Although this approach may require more backup volumes, it will be easier to organise them and to locate files for restoration than with incremental or full volume backup.

Backup Media

407. Magnetic tapes or removable hard disks are required for full disk backup. However, diskettes may be suitable for application backup strategies if the application files are relatively small. Errors in backup copies can obviously have disastrous consequences. The typical backup utilities available on personal computers are basically file copy functions and do not contain the redundancy mechanisms found in some larger systems. For backup purposes, high quality media should be used.

408. Additional assurance of successful backup can be achieved by performing file comparison between the original and the backup copy. Most backup and copying functions provide options for 'verify after write' which

should be selected. In addition, multiple backup copies should be maintained to provide fall back should a media failure or loss of backup occur.

409. Primary backups should be stored close to the equipment on which they may need to be used, with a second backup set stored off-site in order to provide a recovery capability in the event of a major catastrophe at the primary site.

410. Where personal computers are networked it may be possible to arrange for the archiving to be done directly to one or more remote locations. This can provide the physical separate storage necessary for effective disaster recovery.