IMIA Computer Committee

Report on Computer Viruses and the implications for IMIA members

June 1995

Background

There is increasing awareness amongst insurers of the true risks involved from computer viruses. The real value of lost corporate data and the consequential loss due to the time taken for systems to be cleaned and brought back to operating status are hard to estimate as, despite bouts of media publicity, relatively few instances are reported and few insurance claims are thoroughly investigated.

Without detailed analysis it is easy to confuse programming errors, logic bombs and system malfunctions with a virus attack. Even then the vast majority of past and current viruses, correctly diagnosed, are relatively harmless and more of an embarrassment and an inconvenience than a fatal blow to the corporation. However, the threat to corporate data from a truly malicious virus is real enough, resulting in total failure of operations if the correct treatment is not administered. A recent study by Price Waterhouse showed that 15% of Times 1000 firms which suffer a catastrophic failure of computer systems each lost more than £1m. IBM estimate that 70% of all companies subjected to a catastrophic computer incident ceased trading within 18 months.

There is an increasing demand for Information Technology risks of all types to be underwritten, and a recent history of poor insurance results in this area. However, with more education, better underwriting information, better insurance product targeting and growing customer demand, it is believed that there are significant opportunities for profitable business in specific areas of risk in the Computer Insurance market.

This paper attempts to define the technology and the business implications of one such area of risk, the computer virus.

1. So what is a computer virus anyway?

10 years ago the idea of the computer virus belonged to science fiction writing. Although there is now a far greater awareness, due mainly to intense and somewhat over-hyped media attention, there are still users under the impression that computer viruses are biological in nature.

Strictly speaking, a computer virus is the name given to a computer program that has the ability to replicate itself. If all the program does is to make a copy of itself, either on the host computer or on any other computer it comes into contact with, then it's still a virus. In fact, the vast majority of viruses do just this, without causing extensive malicious damage or doing anything else apart from displaying a message. The trouble is that a few of them are definitely nasty in their effects, and as there are so many of them 'in the wild' it is hard to keep up with which ones are benign and which ones are beastly.

You may have also heard of 'Trojans'. If a program does something deliberately nasty, but does not replicate itself, it's a Trojan, not a virus. Of course, some Trojans are the result of viruses themselves (they may be part of the 'payload' of the virus).

Another term for a non-infectious Trojan is a program 'bomb'. These are harder to define, as they could be quasi-legal; for example the computer code which locks you out of your computer application because you haven't paid the latest maintenance fee, just when you're desperately trying to get those urgent management reports generated. In this case the usual result is to pay the maintenance bill and vow to swap your computer software supplier. On the other hand, the Trojan deliberately left behind by the programmer with a grudge against his employer can do untold damage, and will be far harder to work around.

It is perhaps unfortunate that the term 'virus' was used, as the effect on the lay person is to think only in biological terms. However the use of the term is at least understandable if we look at the parallels between the types of biological and the computer viruses.

Computer virus	Biological virus
Attacks particular file types	Attacks particular body cells
Systems can be made immune against known viruses	Immunisation will protect certain cells from infection
A program is infected once only	A cell is not infected more than once
The infected program file is modified to operate differently	The genetic information is modified
The infected program replicates the infectious part	New viruses are grown by the infected cell
There may be a considerable time delay before the effect is apparent	The infected organism may lie dormant for a long time
Virus programs can change themselves to avoid detection	Viruses mutate and may produce other viruses which are totally different

To understand how it is possible for a computer program to act in a similar way to a biological virus, it is first necessary to ensure that we understand some of the specific terms used in computing.

Hardware The simplest definition describes hardware as any part of the computer and its innards that you can touch (with the power off!). Hardware consists of the following:

Processor This performs logical and arithmetic functions

Memory The **working** memory of a computer stores temporary instructions and information. This **R**andom **A**ccess **M**emory is where you put limited information which the computer must access quickly. Information held here needs to be read in when the computer is turned on and at the start of a program, and is lost when the computer is turned off.

Permanent memory is held in **R**ead **O**nly **M**emory (also described as permanent storage). Information held here is 'burned in' to the Permanent Read Only Memory chips by the manufacturer, and cannot be changed (except usually by removing the chip and re-burning it).

Peripherals This term covers all the physical (touchable) devices which are attached, such as modems, printers, screens, keyboard etc.

Mass Storage This is the 'filing cabinet' memory of the computer, which you can add to or delete from yourself. Programs and data are held here on internal (fixed) or removable disks.

Software Software consists of a sequence of instructions to the computer. The computer's operating system, all the application programs and any programs you may write yourself are all **classes** of software.

Operating System This interprets your commands and converts them into instructions for the computer, and provides the program environment by using functions that are stored in the Read Only Memory.

Application Software This describes all the programs (whether bought or written) which make the computer perform useful tasks. Word processors, database programs, accounting, process control applications and computer aided design systems are classes of application software.

Compiler The source (or readable) code of a program is translated into an executable program (a collection of instructions that are understood by the functions held in the permanent storage) by the compiler.

The working memory of a computer (RAM) is managed by the operating system and the application software. The area at the top end of the memory is normally reserved for the operating system, and usually underneath this will be the memory allocated for two or more application programs. The lowest system addresses are under the control of the functions and instructions contained in the permanent memory (ROM) devices.

This arrangement of memory, devices and application software is common across the vast majority of mainframe, mini and PC computers, and hasn't changed appreciably since the advent of commercial computing. It is usual for several application programs to be in working memory at any one time, in addition to the operating system. However, the processor on most computers can only deal with one instruction at a time. There are variations on this, with larger computers having large numbers of processors built in- this gives these types of Central Processing Unit the ability to handle instructions in parallel, although each individual processor is still only doing one thing at a time.

When two or more programs are apparently running at the same time, in actual fact each one is run for a short time before the next program has a computational 'slice' of the action. You will not normally be aware of other programs which are Memory Resident at the same time as the one you are using, unless exceptional demands are made on the processor or peripherals, or a message is sent from the other programs.

From this it is clear that a cleverly written virus program can operate without your knowledge on most of today's computer hardware. Further, it can avoid discovery for as long as it chooses to remain discrete.

However, the virus needs to find a way to load itself into memory in the first place. Innocent or malicious access to the computer system can introduce the virus, perhaps attached to an application program or a Shareware program from an Internet Bulletin Board, or perhaps left behind by a misguided employee. This highlights the need for adequate security measures to be in place around and on all computer systems at all times. It is the best form of defence.

The vast majority of computer software is now distributed to the customer in the form of object code, and not readable source code. An object code file contains instructions in direct machine language which are unintelligible to the average computer user. The change of any bit of this object code file would most likely 'crash' the program.

There are, however, special programs which help these changes to be made. Computer 'hackers' will use these disassemblers to inspect and reverse engineer the code for their own purposes (for instance to change any ownership information contained on a pirate copy of application software).

The computer and most of its operating system will not differentiate between program and data files, and so it is also possible for a program to attempt to disassemble and modify another object file. So, not only can programs change data, they can also change programs. Most application software will actually change itself during the first time you load or run it, to permanently record user and ownership information.

It is a small step from knowing how to write a program that can change other programs, to knowing how to make this program reproduce itself at the same time.

2. An abbreviated History of the Computer Virus

Documented ideas concerning the possible use of worm programs across distributed computer networks date back to 1980. However, reporting of the computer 'virus' first appeared in the popular press following an imaginative news article in the USA in 1985. An apparently innocent attempt to change the system message on starting CP/M micro computers (with the Apple II, CP/M micros were the precursor to the Personal Computing revolution) resulted in the realisation that there was executable code in the 'boot sector' of a floppy disk (the first sector or part of the disk which is looked at by the computer when it is first turned on, so as to load the operating system into memory).

Changing this code enabled the virus code to be loaded into memory alongside the operating system when the machine was turned on. Any time another floppy disk was inserted into the drive the virus was able to infect the new disk directly. When an infected disk was eventually used to 'boot' another computer, the virus could start to spread.

This virus was the first *'boot sector'* virus. It's payload was harmless, being restricted to displaying a simple copyright message on booting up, and was simple to get rid of (you just destroyed the disk). However the following year the first *'file'* virus appeared.

By adding itself to any other executable file, in this case any .COM file it could find, it is possible for a file virus to copy itself when that executable 'host' program is run. The virus will then infect (attach itself to) other programs it finds on the disk, so when the host program is innocently copied and executed on another computer the virus spreads again.

The first known file virus generated a lot of interest in 1986, mainly because it was freely distributed at a computer club conference. Its effects were not harmful, but the ease with which any programmer could pick up ideas from this first demonstration led to a proliferation of viruses and the first intentionally destructive 'Vienna' virus in 1987.

Vienna attached itself to every eighth executable file it found. The next time you executed one of these affected programs the additional code caused the computer to re-boot itself.

Up to this point, viruses were an inconvenience. The user could always restart the computer, and their data was still intact. The biggest danger was unnecessary panic, a delay in working practices and a profit for the increasing number of 'experts' who would clean the system for you. This was about to change.

Fred Cohen's book and research work have received the most attention of any to date. His experiments at the University of Southern California led to him being banned from accessing the computer facilities there. First on a DEC VAX mainframe in 1983 he produced a program called "vd" which succeeded in obtaining all system authorisation codes in less than 1/2 second of processing time, without detection. The following year he produced theoretical work on the propagation speeds of viruses and mathematical proofs that virus detection programs can never be 100% effective.

Despite the negative reactions to Cohen's work, some of it was relevant and novel. He attempted to define the probability of a virus program being developed by chance, and he published code that recurs in today's viruses. He was also at the same place, at the same time that the Lehigh virus was produced. Lehigh was too damaging to become widespread. As with biological viruses, if they kill their host too quickly they don't get a good enough chance to spread, and therefore die out. This however is of little comfort to the host. Lehigh overwrote the file allocation table of hard disks, making data recovery unlikely.

In 1989 the Datacrime and the Jerusalem viruses and the AIDS Trojan created the biggest media panic, as Datacrime (otherwise known as Columbus by the Americans) would hit on a Jerusalem day of Friday 13th. October. In fact, very few occurrences were reported, but the police took it seriously and so did IBM, releasing their own detection program. The Aids Information Disk resulted in the arrest of the author on extortion charges. AIDS triggered a Trojan after a number of computer boots which encrypted all the data on your disk- you were then invited to send money to a Panama box number in order to get the encryption key.

The 'suriv' viruses had already appeared in Israel. These were the first to use the ability of programs to stay resident in memory, even after the host program had been terminated (hence the generic name for Terminate and Stay Resident TSR programs). This ability has been used to great effect by many commercial programs, such as Borland's Sidekick. The suriv virus which escaped 'to the wild' was known as Jerusalem, which deleted any program that was run on a Friday 13th.

The Stoned virus was also memory resident, and probably will remain the most widespread of all. It succeeded in spreading world-wide, as did Jerusalem and Cascade, mainly because of the lack of investment in virus protection devices and policies. Cascade was unusual in that most of the virus code was encrypted, with only a tiny part of the code being used to install the encrypted code. This concept was the beginning of 'polymorphic' viruses, which are designed specifically to beat the anti-virus software suppliers.

Bulgaria and Russia started to produce a number of viruses in 1990 which enormously increased the menace of being infected. Dark Avenger was capable of spreading the virus on just opening any file, and a variant produced occasional subtle data changes on the hard disk. This affected back-ups of data files- if you don't know you have the virus, eventually all your computer back-ups are corrupt. About this time the first virus exchange bulletin board appeared, which encouraged people to experiment with the concept. Soon, 'stealth' viruses were proliferating, and Dark Avenger produced a virus engine, from which anyone could produce their own stealth, polymorphic virus.

Virus detection software was then concentrating on knowing where to look in a data or program file to find the virus 'fingerprint'. They also checked the size of files on your disk, and could then mark for suspicion any files whose size had changed. But then Commander Bomber and Starship viruses made it necessary for scanners to be more thorough. Commander Bomber varies where it stores the virus fingerprint in any file, and Starship only infects files that are being copied from one disk to another so that the size of hard disk files don't change after they are first saved. These new viruses also avoided detection by installing themselves on new partitions on the disk.

Other methods of stealth are employed by some of the more recent viruses. The 'frodo' virus is capable of interpreting the file commands by trapping the interrupt generated by the operating system. It then provides the system with the file information it would have seen in an uninfected file (the way it keeps tag of infected files is to add 100 years to the date stamp of the file). 'Frodo' also changes the interrupt handler to force a jump to its own code, and cleans this change up after it has finished. The 666 virus escapes detection from memory mappers by exactly fitting into the first 512 byte operating system buffer, and the 'Joshi' virus will trap any attempt to investigate the infected area and redirect it elsewhere.

It is unlikely that the current virulent viruses will ever be completely eradicated, and the intellectual challenge and acclaim which virus authors enjoy will ensure that the number of polymorphic, stealth viruses is set to increase. Currently there are over 5,000 known viruses in the wild, and the danger to corporate data integrity should now be evident, requiring all computer installations of whatever type to be vigilant.

By far the worst damage that can be done by the virus writer is to the integrity of corporate data. One simple data change virus performs a search and replace every 39th. full backup on every 39th. occurrence of the number 9 (which is represented in hexadecimal format as 39H). The implications of this are severe, with payroll, invoicing, financial planning and ultimately all backups affected.

Other forms of damage or loss from viruses include slow-down viruses, which progressively utilise more and more of the host computer's resources. In one documented case this type of virus, which slowly propagated more and more apparently genuine batch jobs, caused the replacement of the host computer under the belief that the existing hardware couldn't cope with the company's requirements.

Hunter-killer viruses target particular hardware peripherals, such as certain types of printers. By occasionally sending certain control characters directly to the attached print device it is possible to make the printer appear unreliable. It is possible to directly address the disk controller so that on one make of hard drive the read-write head attempts to move past the end stop, and can only be freed by disassembly. On another make of drive it is possible to use low level instructions to erase control tracks so as to render the disk useless. It cannot even be formatted again.

It is a matter of some surprise that more of these killer viruses have not been issued to date. Certainly they require a better knowledge of specific hardware and devices, are far harder to write effectively and are far more tightly targeted at limited numbers of computer installations. Now suspicions have been aroused, it is perhaps not just science fiction that agents for rogue manufacturers could in future be involved in targeting their competitors hardware.

Call-me viruses can replicate themselves around a network, unobtrusively capturing passwords from sign-on procedures, and physically calling and logging on the virus author at a set time of day. Here, the damage may only be the use of computer time, and the loss of privacy for data files. However, the real cost is that of compromised security, and the potential for malicious damage and theft of data. Further, the replication of the virus allows the author to continue access, even if one of the infected programs is found and all passwords are changed.

Viruses still spread accidentally through the exchange of diskettes, and some instances of inadvertent transmission from software houses have been recorded (most recently from Microsoft themselves). But now awareness of the virus threat is greater, and security procedures are commonly in place at the majority of corporate sites, the main threat is from Network and bulletin board connections, attacks from hackers and employees' mischievous and misguided intentions.

3. Defining the Actual Risks

The preceding section has given some idea of the sort of problems that viruses can cause, and a few pointers on the areas to concentrate in order to reduce the risk of infection. To further define the risks involved, the following should be considered:

- A survey of computer managers published in 1994 showed that 20% of respondents had experienced a computer 'disaster' within the last 12 months. A third of these were caused deliberately, either by fraud, malice or misuse. Viruses were the reason for a fifth, another fifth were caused by flood, fire or lightning, and most of the remainder were caused by software or hardware failure (Computing Services Association).
- 60% of U.K. firms do not have insurance against employee negligence or wilful abuse of their computer systems. 85% are not covered against the software failure of their own systems. Only 9% have cover for loss of data. 25% of all computer sites have no means of auditing their own computer usage (National Audit Commission).
- When disaster does strike a computer system, 43% of European companies are left with no recovery plan at all (IBM).
- The majority of the disaster recovery plans that do exist are worthless because they have not been properly tested. In the case of virus attack, the back-ups are usually infected, making them useless.
- Because most corporations now insist on basic virus checking operations (using third party software), only 2 PC's per 1000 are virus infected (it had been forecast that 1/4 of all PC's would have been infected by the end of 1994).
- The most common host for virus transmission is via illegal or unauthorised software copying ('pirate' software, which costs the computer software industry a loss of an estimated $12bn. world-wide). In the USA, 35% of software is pirated (accounting for $2.2bn. in lost sales). The 'most illicit' countries for software piracy are Pakistan, United Arab Emirates, Kuwait, Russia, Malaysia and Peru (The Economist).

- Poor internal security is largely to blame for the rise in computer crime. Of 1000 European companies investigated, losses due to computer fraud were claimed to cost more than $6m, with a reported 261 cases of deliberate virus damage costing an average $1,500 each (National Audit Commission).
- Robert Morris was the first person to be successfully convicted of planting a virus under the USA Computer Fraud and Misuse Act. In November 1988 his 'viral worm' corrupted and brought down 6000 Internet host computers, including a NASA mainframe. The actual damage caused was before the court at $1000, but down time and labour costs for this case have been estimated to be more than $5m. There is currently a case in British courts where the first conviction has been successfully brought for planting a computer virus (the judge has called for 'expert opinion' on the value of damages incurred before sentencing).

So what are the actual financial implications to insurers of these risks?

As the following table shows, the actual returns of claims experience implies that the effects of successful claims from viruses are not particularly significant.

Reporting Country	Estimated % of Market	Reported Total Claims '94 No.	Reported Total Claims '94 $Value	No. Reported due to Viruses	$ Value of Virus Claims	% of Total Claim Value
The Netherlands	75%	2769	6.1m	2	$4500	0.1
United Kingdom	5%	3408	14.65m	0	0	0
Austria		3230	4.7m			
France	5%	432	1.3m	0	0	0
Spain			2.4m	nk		
South Africa	100%	4089	4m	0	0	0
Sweden	40%		0.1m	nk		

this table will be more complete following returns by the end of June

However rosy a picture this paints there is no doubt that a number of virus attacks which have resulted in claims are not categorised by insurers, and significant numbers that do not result in a claim for whatever reason. It is difficult to accurately value the direct and indirect losses in these cases, and there are two significant cases involving virus damage in the UK and USA courts at present awaiting confirmation of losses. It is further known that four claims of more than $100k in the UK should have been ascribed at least partially to virus damage instead of being uncategorised.

Insurers have been fortunate to date in their exposure to virus claims. Even allowing for the reluctance of insured and insurer alike to admit to the true value of virus damage (as this would publicise the breach in security), it is limited at present. On average, physical hardware and software theft account for 75% of total claims, with virus specifically nominated at less than 1%. However, the majority of returns confirm the suspicion that types of physical damage and theft are well categorised, but other areas such as virus, contaminants and negligence are still categorised together under 'Other Causes' which count as the third largest percentage of total claims *(so far)*.

1994 Reason for Claim	Total Claims Value $	Number of Claims
Theft	38m	7000
Breakdown	6m	
Storm/Flood	1.8m	
Electrical fault	1.2m	
Lightning	0.9m	
Fire		
Malicious damage	0.5m	
Contaminants		
Impact damage		
Negligence		
Virus		
Other	4.2m	1950

Contributing countries: list......... this table to be completed by June end.

Insurers are presently finding difficulty in using their loss experiences to quantify risk in this area as they usually do not have the specialised knowledge necessary, nor do they normally have the opportunity of an effective post-mortem following a virus attack. Better breakdown of claims by type is required, as are effective proposal or survey forms to help pinpoint high risk features.

Further, risks can be dramatically different depending on the industry type, as the following table shows.

Type of	No. in	% with	Number	of cases			
Organisation	Sample	Incidents	Virus	Fraud	Sabotage	Data Theft	Hacking
Local Government	290	41%	85	63	4	6	5
Health	334	35%	69	11	0	7	10
Central Government	24	46%	40	21	0	0	3
Finance/Insurance	87	45%	17	4	0	2	2
Education	58	36%	11	0	3	4	8
Manufacturing	125	20%	10	2	3	4	6
Other Commercial	155	35%	29	7	6	8	10
Total	1073	36%	261	108	16	31	44
Direct Losses		£3.2m	£30k	£2.9m	£66k	£186k	£9k
Indirect Losses		£625k	£224k	£137k	£39k	£36k	£29k
Total Losses		**£3.8m**	**£254k**	**£3m**	**£105k**	**£222k**	**£38k**

source: U.K. Audit Commission October 1994 survey.

Although this survey was voluntary and restricted to the UK, it represents returns from over a fifth of the sample requests. It should be noted that these results were completed by the heads of Information Technology departments, who may well have had little input on the decision to insure various risks.

Statistically the number and quality of replies give fairly high confidence levels in extrapolating these figures out (note that physical theft of hardware is not included here). Knowledge of relative environmental factors would suggest similar results across other industrialised countries.

A great deal remains to be done to raise the customer's awareness of the true risks to their business from data and computer corruption, and to ensure that these risks are balanced with appropriate insurance. It is important that both the insurer and the insured understand the true risks, so that more appropriate policies may be sold into a more secure customer environment.

4. Strategies for Better Underwriting Results

The development of techniques to systematically evaluate every component of risk in computer insurance is a specialised task, but the results will enable the insurer to set more accurate premium levels, and to decline proved high risk situations if appropriate.

The initiation and better use of survey forms is invaluable at the outset, but the required detail can mean that the survey or proposal form becomes an obstacle to selling the cover.

The insured's existing protection strategies against computer risks usually start with taking out insurance. Measures to control access to the computer site then follow, and specific virus risks are usually addressed by the purchase of a proprietary software package to hunt and destroy known viruses by analysing existing software and data. Finally the company attempts to provide better education on risk management for the users.

A better method of reducing computer risks of all types is to start by encouraging better working practices at the computer site, and to ensure that the following actions are taken:

- Identify the systems that are at risk.
- Properly assess the opportunities for misuse, and establish steps to avoid this.
- Agree and assign responsibility for overall security to experienced staff, and further ensure that responsibility for specific areas of data are agreed.
- Enforce the effective use of passwords.
- Control physical access to computer systems.
- Make sure that hardware and software maintenance contracts are competent.
- Always ensure that key duties are divided up between personnel.
- Rigorously control access across Wide Area Networks and all modem access.
- Ensure that computer staff take up their holiday entitlement.
- Install monitor and audit systems that identify unusual working patterns.
- Take daily, weekly and monthly back-ups.
- Properly test your back-up procedures regularly.

- Only purchase software from established computer software suppliers.

- Document and publish procedures for use in case of virus detection:
  1. Don't panic! Call an authorised expert for advice- you may not need to reformat all your disks ant reconstitute the whole system. However, if you do:
  2. Turn the system off to prevent spread and kill memory resident.
  3. Disconnect all data lines to printer, modems and networks.
  4. Ensure all disks are write protected.
  5. Reboot using the original operating system disks.
  6. Back up existing data and programs for expert analysis later.
  7. Re-format all disks.
  8. Restore software using original disks, which will have been virus checked.
  9. Check data backups for consistency (this may dictate recovery from old data).
  10. If not already used, install anti virus software and perform extensive tests.
  11. If there is no capability in house, send the affected disks to a recognised virus software facility for analysis and to support any insurance claim.

- Check all computers for viruses at power-up.

- Check all disks from any source for viruses.

- Build an environment where computer staff can feel responsible and trusted.

- Prohibit the loading of games and any other unauthorised software.

- Properly screen staff for jobs involving secure data, and take up all references.

- Ensure that staff are aware of the policies and procedures, the reasons for them and the penalties for breaking them.

- Build in safeguards against unauthorised access to personal data: discourage general browsing around computer data.

- Regularly audit the policies and procedures, safeguards and controls: strengthen the good ones and get rid of the unnecessary ones.

- If possible, restrict Internet and modem access to one stand-alone computer.

- Insure against known risks (theft, physical damage, fraud, misuse, sabotage, virus).

The computer virus predominantly threatens networks of PC's running DOS or Windows, but in fact all modern hardware and operating systems are at risk to some extent. Apple Macintosh sites, UNIX machines and central mainframe systems are all at risk, as are OS/2 and Windows NT systems. Although there are no known viruses on the NT, and the one

OS/2 virus in the wild is not particularly dangerous, these and other operating systems capable of supporting DOS networks can act as hosts. A virus will be successfully installed if an OS/2 or NT system is accidentally booted with a DOS disk containing a boot sector virus, even though the most likely result will be an obviously corrupt system.

The use of third party, properly maintained and upgraded software products which run as normal DOS programs will be the most effective way to hunt and destroy viruses for the foreseeable future. Hardware devices built in at the time of PC manufacture to add virus protection to the BIOS will be of no use when 32bit operating systems are loaded which replace the BIOS anyway.

There used to be a significant number of companies offering anti virus software, but the difficulties of keeping on top of new viruses and making the software products acceptable to the customer has seen the numbers fall to about 15 recognised suppliers. S&S International (Dr. Solomon's) and Sophos provide software for the greatest range of systems, covering Windows, DOS, DEC VMS and UNIX Open, NT and OS/2. McAfee Associates cover DOS, Windows, OS/2 and NT, and the rest of the suppliers concentrate mainly on DOS and Windows.

While there is some difference in effectiveness in hunting viruses, there is a much greater difference in usability and speed of searching. It is not the purpose of this paper to recommend particular suppliers in this area, but it is advised that proper advice is taken over the selection of this software. Due consideration must be given to reputation, performance, maintenance and suitability to the environment, in addition to the cost of multiple licenses where necessary. It may be best for the virus checking software to be installed on each and every computer you use, and most of the products are designed to be used this way. However, in certain controlled circumstances it may be better to ring fence your installations following a thorough virus check, and prohibit any changes or updates that have not been checked by a dedicated and isolated machine.

It is worth stating that although anti virus software is an imperative nowadays, total reliance on this form of defence is misplaced. Remember that people spread viruses, not computers.